МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ЖИТОМИРСЬКИЙ ВІЙСЬКОВИЙ ІНСТИТУТ ІМЕНІ С.П. КОРОЛЬОВА

ПІЛЬКЕВИЧ І.А.
ЛОБАНЧИКОВА Н.М.
МОЛОДЕЦЬКА К.В.

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

НАВЧАЛЬНИЙ ПОСІБНИК

Житомир
Вид-во ЖДУ ім. І. Франка
2015

УДК 681.51:004.056
ББК 32.965+32.973.202 я73
З 75

Рекомендовано до друку вченою радою Державного університету телекомунікацій (протокол № 3 від 29 жовтня 2014 року).

Рецензенти:

Ю.О. Подчашинський – завідувач кафедри комп'ютеризованих систем управління та автоматики Житомирського державного технологічного університету, д.т.н., доцент

В.М. Котенко – завідувач кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова, к.т.н., доцент

З 75 Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

У навчальному посібнику розглядаються сучасні напрямки забезпечення захисту інформації в автоматизованих системах управління. Представлено теоретичні основи та понятійних апарат безпеки інформаційних систем та технологій. Розглянуто питання вразливості, організаційно-правового забезпечення захисту інформації. Викладаються технічні, криптографічні, програмні моделі, методи, засоби та технологій побудови сучасних систем захисту інформації. Виклад матеріалу з прикладним спрямуванням допоможе студентам освоїти матеріал дисципліни "Захист інформації в автоматизованих системах управління" з метою набуття необхідних знань, вмінь та компетенцій. Навчальний посібник призначений для студентів, що навчаються за напрямом 6.050201 "Системна інженерія".

Укладачі: доктор технічних наук, професор **І.А. Пількевич**; кандидат технічних наук, доцент **Н.М. Лобанчикова**; кандидат технічних наук, доцент **К. В. Молодецька**.

ББК 32.817

ЗМІСТ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСУ – автоматизовані системи управління
БД – база даних
ІКС – інформаційно-комунікаційна система
ІС – інформаційна система
ДПБ – дискреційна політика безпеки
КІ – карти ідентифікації
КЗЗ – комплекс засобів захисту
КНОІ – канал несанкціонованого отримання інформації
МПБ – мандатна політика безпеки
НСД – несанкціонований доступ
ОС – операційна система
ПБ – політика безпеки
ПВЧ – псевдовипадкові числа
ПЗ – програмне забезпечення
ПЗП – постійний запам’ятовуючий пристрій
РПБ – рольова політика безпеки
СВК – система з відкритим ключем
СЗІ – система захисту інформації
СКБД – система керування базами даних

ВСТУП

На сучасному етапі розвитку науки і техніки захист інформації перетворюється на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження як автоматизованих систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру. Важливим завданням є широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, введення електронних паспортів і медичних карт, студентських квитків та залікових книжок. Все більше державних установ і приватних підприємств переходять на електронний документообіг, який вимагає юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій вимагає захисту інформації. Усі ці та багато інших задач покликані вирішувати різноманітні методи, засоби і технології захисту інформації.

Мета навчальної дисципліни закласти термінологічний фундамент, навчити студентів правильно проводити аналіз загроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в АСУ з урахуванням сучасного стану і прогнозу розвитку методів, систем та засобів здійснення загроз зі сторони потенційних порушників.

Завданнями дисципліни є ознайомити студентів з основними уявленнями про основні загрози інформаційної безпеки АСУ, навчити їх самостійно обирати та використовувати сучасний методи та засоби захисту інформації, виконувати оцінку якості функціонування системи захисту інформації в АСУ.

У результаті вивчення навчальної дисципліни студент повинен ***знати*****:** загальне поняття та характеристики інформації, загальні вимоги до захисту інформації в АСУ; поняття та основні складові інформаційної безпеки; існуючі моделі загроз та порушника безпеки інформації в АСУ, причини порушення безпеки; класифікацію засобів забезпечення безпеки в АСУ, організаційні та технічні заходи забезпечення захисту інформації; принципи захисту інформації від несанкціонованого доступу в АСУ, методи аутентифікації та ідентифікації користувачів АСУ, методи контролю доступу; криптографічні методи захисту

інформації, їх класифікація, особливості застосування; поняття електронного цифрового підпису, особливості розподілу ключів в АСУ; організаційні принципи побудови систем захисту інформації, особливості їх реалізації, методи побудови захищених АСУ; поняття політики безпеки, класифікація політик безпеки, особливості реалізації в АСУ; основні поняття стеганографії як науки про приховання передачі даних; методи та засоби оцінки ефективності СЗІ АСУ; ***вміти*:** виконувати організацію технічного захисту інформації в серверних приміщеннях; реалізовувати організацію безпеки даних на рівні сумісного використання; проводити реалізацію алгоритмів шифрування та дешифрування даних; визначати структуру системи захисту інформації АСУ, розраховувати міцність захисту інформації; виконувати адміністрування СКБД MS SQL Server; проводити багатокритеріальний вибір варіанту системи захисту інформації в АСУ; проводити розрахунок інтегральних показників ефективності системи захисту інформації АСУ.

Вибір засобів захисту інформації в автоматизованих системах – складна задача, при розв'язанні якої потрібно враховувати всі можливі дії щодо порушення роботи інформаційної системи, вартість реалізації різних заходів та засобів захисту і наявність всіх зацікавлених сторін. Сучасна наука має в своєму розпорядженні методи та інформаційні технології, що дозволяють вибрати таку сукупність засобів захисту, яка забезпечить максимізацію міри безпеки інформації при даних витратах або мінімізацію витрат при заданому рівні безпеки інформації.

У навчальному посібнику викладені теоретичні та практичні аспекти захисту інформації в АСУ. Викладаються технічні, криптографічні, програмні моделі, методи, засоби та технологій побудови сучасних систем захисту інформації. Виклад матеріалу з прикладним спрямуванням допоможе студентам освоїти матеріал дисципліни "Захист інформації в автоматизованих системах управління" з метою набуття необхідних знань, вмінь та компетенцій. Навчальний посібник призначений для студентів, що навчаються за напрямом 6.050201 "Системна інженерія".

При підготовці навчального посібника використано досвід та напрацювання авторів в галузях інформаційної безпеки та автоматики та управління, математичного моделювання та прогнозування, а також результати численних досліджень провідних вчених сьогодення, навчально-методичні та наукові видання професіоналів Житомирського військового інституту імені С.П. Корольова.

РОЗДІЛ 1. ПОНЯТТЯ ІНФОРМАЦІЇ, КОМПЛЕКС ДЕРЖАВНИХ СТАНДАРТІВ УКРАЇНИ

СКЛАД ЗМІСТОВНОГО МОДУЛЯ

Лекція 1. Поняття інформації, комплекс державних стандартів України
1.1. Інформація, її види і властивості.
1.2. Форми представлення інформації в АСУ.
1.3. Особливості інформації.
1.4. Сучасний стан питання захисту інформації.
1.5. Нормативно-правове забезпечення захисту інформації в АСУ.
Контрольні питання
Література для самопідготовки
Лекція 2. Загрози безпеки інформації в АСУ
2.1. Джерела загроз інформаційної безпеки.
2.2. Системна класифікація і загальний аналіз загроз безпеки інформації.
Контрольні питання
Література для самопідготовки
Лекція 3. Основні моделі теорії захисту інформації в АСУ
3.1. Моделі загроз і потенційного порушника.
3.2. Причини порушення безпеки.
Контрольні питання
Література для самопідготовки
Лекція 4. Організаційно-технічні заходи забезпечення захисту інформації в АСУ
4.1. Напрями забезпечення безпеки інформації.
4.2. Основні види технічних каналів і джерел витоку інформації.
4.3. Способи запобігання витоку інформації по технічним каналам.
Контрольні питання
Література для самопідготовки
Питання, що опрацьовуються студентами самостійно

ЛЕКЦІЯ 1. ПОНЯТТЯ ІНФОРМАЦІЇ, КОМПЛЕКС ДЕРЖАВНИХ СТАНДАРТІВ УКРАЇНИ

1.1. Інформація, її види і властивості.
1.2. Форми представлення інформації в АСУ.
1.3. Особливості інформації.
1.4. Сучасний стан питання захисту інформації.
1.5. Нормативно-правове забезпечення захисту інформації в АСУ.

1.1. Інформація, її види і властивості

В умовах широкого застосування обчислювальної техніки і засобів обміну інформацією поширюються можливості її просочення та несанкціонованого доступу до неї зі злочинною метою. Особливо уразливими сьогодні залишаються незахищені системи зв'язку, в тому числі обчислювальні мережі. Інформація, циркулююча в них, може бути незаконно змінена, викрадена або знищена. Останнім часом у засобах масової інформації з'явилося безліч сенсаційних повідомлень про факти злочинних впливів на автоматизовані системи обробки, зберігання і передачі інформації, особливо в банківській діяльності.

За деякими даними, в промислово розвинених країнах середній збиток від одного злочину в сфері комп'ютерної інформації близький до 450 тис. дол., а щорічні сумарні втрати в США і Західній Європі, за даними, що наводять Гайкович В. та Прешин А., досягають 100 млрд. і 35 млрд. доларів відповідно. В останні десятиріччя зберігалася стійка тенденція до зростання збитків, пов'язаних з злочинністю в сфері комп'ютерної інформації. В пресі та літературі наводиться багато подібних прикладів.

Комерційним і фінансовим установам доводиться реалізовувати широкий набір заходів, щоб захистити себе від таких злочинів. Наслідки недооцінки питань безпеки можуть виявитися вельми сумними. Досить згадати про великі суми, викрадені за допомогою підроблених авізо. На жаль, досвід західних фірм дає небагато підстав сподіватися, що цей перелік не буде продовжений у майбутньому в нашій країні. Тому питанням інформаційної безпеки приділяється все більше уваги.

З метою протидії злочинам у сфері комп'ютерної інформації або зменшення збитків від них необхідно грамотно вибирати заходи і засоби забезпечення захисту інформації від просочування та несанкціонованого доступу до неї. Необхідно знати також основні законодавчі положення в цій області, організаційні, програмно-технічні та інші заходи забезпечення безпеки інформації.

Актуальність даної проблеми пов'язана із зростанням можливостей обчислювальної техніки. Розвиток засобів, методів і форм автоматизації процесів обробки інформації і масове застосування персональних комп'ютерів роблять інформацію більш уразливою. У всіх аспектах забезпечення захисту інформації основним елементом є аналіз можливих дій щодо порушення роботи автоматизованих систем.

Основними чинниками, які сприяють підвищенню її уразливості, є:

– збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою комп'ютерів;

– зосередження в базах даних інформації різного призначення і різної приналежності;

– розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи та масивів даних;

– ускладнення режимів роботи технічних засобів обчислювальних систем;

– обмін інформацією в локальних та глобальних мережах, в тому числі на великих відстанях.

Поняття «інформація» сьогодні вживається досить широко і різнобічно. Важко знайти таку область знань, де б воно не використовувалося. До середини XX ст. **інформація** трактувалась які відомості, які передаються людьми усним, письмовим або іншим способом. Після появи електронно-обчислювальним машин дещо змінилося трактування поняття інформації. Там під **інформацією за Шеноном** (ентропійний підхід, американський математик Д.Є. Шенон) почали розуміти зменшення міри невизначеності знання про який-небудь об'єкт, систему, процес або явище, як зміну невизначеності стану самого об'єкта, системи, явища, процесу.

В цей час з'являється і загальнонаукове трактування поняття **інформації**, як зміни обсягу та структури знання сприймання системи. Тут, сприймальна система розуміється не лише як сама людина або її похідні (колектив, суспільство), але й будь-яка система, наприклад, біологічна клітина, що є носієм генетичної інформації.

Згідно ISO/IEC 17799:2000, **інформація** – це майно (або активи), яке, подібно до інших важливих ділових активів, має цінність для організації, отже, має бути захищене відповідним чином.

Згідно Закону України «Про інформацію», **інформація** – це документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі.

Відомо, що інформація може мати різну форму, включаючи дані, які закладені в комп'ютерах, записки, досьє, формули, креслення, діаграми, моделі продукції і прототипи, дисертації, судові документи й ін. Інформація характеризується життєвим циклом, який можна представити такими складовими (рис.1.1):

– *одержання інформації* – це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою;

– *обробка інформації* – вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних;

– *використання інформації* – це задоволення інформаційних потреб громадян, юридичних осіб і держави;

– *зберігання інформації* – це забезпечення належного стану інформації та її матеріальних носіїв;

– *знищення*;

– *оновлення* – формування інформації в джерелі інформації.

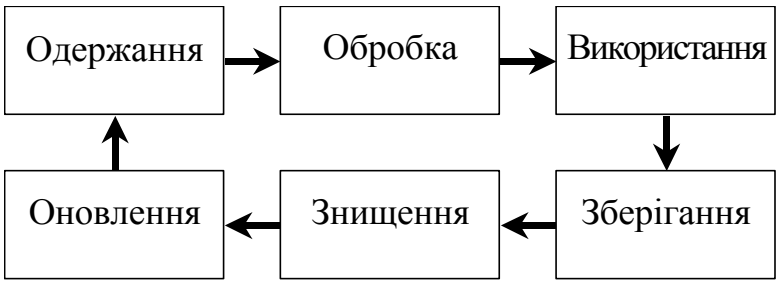

Рис. 1.1. Життєвий цикл інформації

Разом з терміном «інформація» вживається термін «**дані**». Від інформації дані відрізняються конкретною формою подань і є певною підмножиною, визначеною метою та завданнями збору й обробки інформації. Наприклад, дані про співробітників якої-небудь організації у вигляді формалізованих облікових карток кадрового підрозділу містять лише певний перелік необхідних відомостей, на відміну від величезної кількості відомостей, що характеризують кожну конкретну людину.

Можна виділити **неструктуровану** та **структуровану** форми представлення даних. Прикладом неструктурованих форми є зв'язний текст, графічні дані у вигляді фотографій, малюнків та інших неструктурованих зображень. Прикладами структурованих даних є анкети, таблиці, графічні дані у вигляді креслень, схем, діаграм.

Інформація завжди була, є і буде найважливішим із комунікативних ресурсів. Відомий біржовий гравець Натан Ротшильд говорив: «**Хто володіє інформацією, той володіє світом**».

Як і всякий продукт, інформація має споживачів, які потребують її, і тому володіє визначеними споживчими якостями. Також інформація має своїх власників або виробників.

1.2. Форми представлення інформації в АСУ

На світовому ринку інформації прийнято розрізняти наступні **основні сектори**, які також характерні й для України:

а) сектор ділової інформації;
б) сектор юридичної (нормативної) інформації;
в) сектор інформації для фахівців;
г) сектор соціально-побутової (сервісної) інформації;
д) сектор технічних і програмних засобів.

Підприємцеві, в тому числі і соціально-культурної сфери, потрібна інформація із всіх секторів, але успіх його діяльності визначається насамперед своєчасним використанням ділової (фахової) інформації. Сучасний інформаційний ринок даних можна розділити на кілька основних секторів (рис.1.2).

Рис. 1.2. Сучасний інформаційний ринок даних

Постійно зростаюча складність і динамічність виробничих, економічних і соціально-економічних систем, великі розміри цих систем, складність їх зв'язків і взаємозв'язків, колосальні обсяги обчислювальних робіт при плануванні, прогнозуванні і прийнятті управлінських рішень створюють підстави для широкого впровадження інформаційних технологій в практику повсякденного життя фахівців різних сфер діяльності. Інформаційні технології сьогодні представлені великою різноманітністю як по інтелектуальному і системотехнічному складу, так і за областями застосування і організаційними формами функціонування. При цьому в різних сферах діяльності є місце і простим, і складним інформаційним системам.

Прийняті рішення повинні ґрунтуватися на достовірній, поточній і прогнозованій інформації, аналізі всіх факторів, що роблять вплив на рішення, з урахуванням передбачення його можливих наслідків.

Керівники зобов'язані постійно й всебічно вивчати інформацію, що надходить для підготовки й прийняття на її основі управлінських рішень, які необхідно погоджувати на всіх рівнях внутрішньофірмової ієрархічної піраміди керування. У процесі управлінської діяльності інформація стала більш важливим ресурсом, ніж матеріальні, енергетичні, трудові та фінансові ресурси.

Для проведення якісного аналізу наявних інформаційних ресурсів дамо визначення поняттю «**інформаційні ресурси**». Відповідно ЗУ «Про інформацію»: «До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення».

За змістом інформація поділяється на такі види:

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

Згідно ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» визначається:

інформація з обмеженим доступом – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами;

таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю;

конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. До *інформації з обмеженим доступом* не можуть бути віднесені такі відомості:

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

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

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

4) про факти порушення прав і свобод людини і громадянина;

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

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

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

а) форма 1 – для роботи з секретною інформацією, що має ступені секретності «особливої важливості», «цілком таємно» та «таємно»;

б) форма 2 – для роботи з секретною інформацією, що має ступені секретності «цілком таємно» та «таємно»;

в) форма 3 – для роботи з секретною інформацією, що має ступінь секретності «таємно».

Діють такі терміни дії допусків: для форми 1 – 5 років; для форми 2 – 7 років (абзац сьомий частини першої статті 22 із змінами, внесеними згідно із Законом N 2432-VI (2432-17) від 06.07.2010); для форми 3 – 10 років (абзац восьмий частини першої статті 22 із змінами, внесеними згідно із Законом N 2432-VI (2432-17) від 06.07.2010).

1.3. Особливості інформації

Особливості інформації:

– нематеріальність (не має маси, енергії, тощо);

– передається та зберігається на матеріальних носіях (книги, диски, флешки, папір та ін.);

– будь-який матеріальний об'єкт містить інформацію про самого себе або інший об'єкт.

Інформації притаманні такі властивості:

1. *Інформація, якщо вона міститься на матеріальному носієві, доступна людині*.

2. *Інформація має цінність*. Цінність інформації визначається мірою її корисності для власника. Володіння дійсною (достовірною) інформацією дає її власникові певні переваги. Інформація, що спотворено передає дійсність (недостовірна) інформація, може завдати власникові значного матеріального та морального збитку. Якщо інформація викривлена зумисне, то її називають дезінформацією.

3. *Цінність інформації змінюється в часі*. Як правило цінність інформації з часом зменшується. Залежність визначається таким виразом:

$$C(t) = C_0 e^{-2,3t/\tau},$$

де C_0 – цінність інформації в момент її виникнення (здобуття); t – час від моменту виникнення інформації до моменту визначення її вартості; τ – час від моменту виникнення інформації до моменту її старіння.

4. *Інформація купується і продається*. Інформацію доцільно розглядати як товар, що має певну цінну. Ціна як цінність інформації, пов'язана з користю інформації для конкретних людей, організацій, держав. Інформація може бути коштовною для її власника, але не становити цінність для інших. В цьому випадку інформація не може бути товаром. Інформація може бути отримана трьома шляхами: проведення наукових досліджень; купівлею інформації; протиправним здобуттям інформації.

5. *Складність об'єктивної оцінки кількості інформації*. Існує кілька підходів до виміру кількості інформації:

– ентропійний підхід (кількість інформації оцінюється зменшенням в одержувача невизначеності (ентропії) вибору або зменшення очікування подій після здобуття інформації);

– тезаурус ний підхід (запропонований Ю.А. Шрейдером). Тезарусний підхід заснований на розумінні інформації як знань. Кількість інформації, здобутої людиною з повідомлення, можливо оцінити мірою зміни її знань);

– практичний підхід (на практиці кількість інформації вимірюють за об'ємом – сторінки, біти, байти).

У результаті копіювання без зміни інформаційних параметрів носія кількість інформації не змінюється, а ціна знижується.

1.4. Сучасний стан питання захисту інформації

Широкомасштабне використання обчислювальної техніки, збільшення обсягів інформації і розширення кола користувачів телекомунікаційних та інших територіально-розподілених АС обробки інформації приводять до якісно нових можливостей несанкціонованого доступу до інформації, що обробляється. Тому питання безпеки інформації – є важливою частиною процесу впровадження нових інформаційних технологій в усі сфери життя суспільства.

Під *інформаційною безпекою* будемо розуміти такий стан певної системи, за якого вона, з одного боку здатна протистояти дестабілізуючій дії зовнішніх і