Законодавча, наукова та нормативно-методологічна база

Законодавчі заходи щодо ЗІ-ї полягають у виконанні чинних у державі або у введенні нових законів, положень, постанов та інструкцій, які регулюють юридичну відповідальність посадових осіб, користувачів та обслуговуючого технічного персоналу за витік, втрату або модифікацію довіреної йому інформації, яка підлягає захисту, у тому числі за спроби виконувати аналогічні дії за межами своїх повноважень, а також відповідальність сторонніх осіб за спробу навмисного несанкціонованого доступу до інформації.

*Мета законодавчих заходів* – це попередження правопорушень та покарання порушників

Україна намагається не відставати від вимог сьогодення, тому у нашій державі на даний час прийнято ряд законодавчих актів та нормативних документів, які регламентують діяльність у сфері ЗІ. В повній мірі законодавче забезпечення врегульовано лише для державної таємниці. А для інших категорій інформації в чинних актах існують лише декларативні норми.

Основними законодавчими актами та нормативними документами, що регламентують діяльність у сфері ЗІ є:

* *Концепція(основи) державної політики національної безпеки України*. 18 липня 1995р. Цим документом закладаються основи концептуального змісту державної політики національної безпеки. В концепції визначено головні об’єкти національної безпеки(громадянин, суспільство і держава), також в концепції визначені основні принципи забезпечення НБУ.
* Закон України про Інформацію. 2 жовтня 1992р. Даний закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію у всіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, а також захищає особу та суспільство від неправдивої інформації. Суб’єктами інформаційних відносин є громадяни України, юридичні особи та держава.

Згідно даного закону режими доступу до інформації – це передбачена правовими нормами методика одержання, використання, поширення та зберігання інформації.

За *режимом доступу* інформація поділяється на: відкриту та інформацію з обмеженим доступом. З ОД інформація поділяється на конфіденційну і таємну. **Конфіденційна інформація** – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюється за їх бажанням відповідно до передбачених ними умов. До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству та державі.

**Право власності на інформацію** – це врегульований законом суспільні відносини, щодо володіння, користування та розпорядження інформації.

* Закон України …. 21 січня 199?р. Цей закон регулює суспільні відносини, пов’язані із віднесенням інформації до державної таємниці засекречуванням, розсекречуванням їх матеріальних носіїв, та охороною державної таємниці з метою захисту НБУ.

**Державна таємниця** – це вид таємної інформації, що охоплює відомості у сфері охорони, економіки, науки і техніки, зовнішніх відносин державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди НБУ та які визнані у порядку, встановленому цим законом державною таємницею і підлягають охороні держави.

Віднесення інформації до державної таємниці – це процедура прийняття(державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з встановлення ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди НБУ у разі розголошення цих відомостей.

**Гриф секретності** – це реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації

* Закон України про Захист інформації в автоматизованих системах. 5 травня 1994р. Метою закону є встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання прав власності громадянина України та юридичних осіб на інформацію та права доступу до неї, а також встановлення чинним законодавством обмеження на доступ до інформації. Дія закону поширюється на будь-яку інформацію, що обробляється у автоматизованих системах.

**Автоматизована система** – це система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки, засоби обчислювальної техніки і зв’язку, а також методи і процедури та програмне забезпечення. Інформація в АС – це сукупність усіх даних і програм, які використовуються в АС, незалежно від засобу їх фізичного і логічного представлення.

**Обробка інформації в АС** – це вся сукупність операцій, що здійснюється за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних.

**Захист інформації** – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

**Несанкціонований доступ** – це доступ до інформації, що здійснюється з порушенням встановлених АС правил розмежування доступу.

**Розпорядник АС** – це фізична або юридична особа, яка має право розпоряджання АС за угодою з її власником або за його дорученням

**Персонал АС** – це фізичні особи, яких власник АС або уповноважена ним особа, чи розпорядник АС визначили для здійснення функцій управління та обслуговування АС.

**Користувач АС** – це фізична або юридична особа, яка має право використання АС за угодою з розпорядником АС.

**Порушник** – це фізична або юридична особа, яка навмисно чи ненавмисно здійснює неправомірні дії щодо інформації в АС, або щодо самої АС.

**Втрата інформації** – це дія, в наслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому доступі.

**Витік інформації** – це результат дії порушника в наслідок якої інформація стає відомою суб’єктам, що не мають права доступу до неї.

**Підробка інформації** – це навмисні дії, що призводять до перекручення інформації, яка повинна зберігатися або оброблятись в АС.

**Блокування інформації** – це дії, що призводять до припинення доступу до інформації

**Порушення роботи АС** – це дії або обставини, які приводять до спотворення процесу обробки інформації

* *Закон України про науково-технічну інформацію.* 25 червня 1993р. Законом регулюються правові та економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва у цій сфері. Дія закону поширюється на підприємства, установи та організації, незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації. Дія закону не поширюється на інформацію, що містить державну та іншу таємницю, яка охороняється законом
* *Указ президента України від 10 квітня 2000 року про «Заходи щодо захисту інформаційних ресурсів держави»*
* *Концепція технічного захисту інформації України,* 8 жовтня 1997р.
* *Положення про технічний захист інформації в Україні,* 27 вересня 1999р.
* *Положення про контроль та функціонування системи технічного захисту Інформації*
* *Положення про державну експертизу у сфері технічного захисту Інформації*
* *Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю в автоматизованих системах*
* *Положення про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів, системи технічного ЗІ*
* *ДСТУ 3396 0-91 «Захист інформації. Технічний захист інформації. Основні положення»*
* *ДСТУ 33961-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт»*
* *ДБМ А.2.2-2-96 «Проектування. Технічний ЗІ. Загальні вимоги до організації, проектування та проектної документації для будівництва»*
* *Тимчасове положення про категоріювання об’єктів*
* *Загальні положення щодо ЗІ в КС від несанкціонованого доступу, НД ТЗІ 1.1-002-99*
* *НД ТЗІ 1.1-003-99, «Термінологія у галузі ЗІ в КС від НСД»*
* *НД ТЗІ 1.4-001-2000, «Типове положення про службу ЗІ в АС»*
* *НД ТЗІ 1.6-001-96, «Правила побудови, викладення, оформлення та позначення нормативних документів системи ТЗІ»*
* *НД ТЗІ 2.1-001-2001, «Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення»*
* *НД ТЗІ 2.5-004-99, «Критерії оцінки захищеності інформації в КС від НСД»*
* *НД ТЗІ 3.6-001-2000, «Технічний захист інформації. КС. Порядок створення комплексної системи ЗІ в АС»*
* *Звід відомостей що становлять державну таємницю*
* *Інструкція про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, що здійснюють підприємницьку діяльність у галузі криптографічного захисту, конфіденційної інформації, що є власністю держави, затверджена наказом Департаменту спеціальних телекомунікаційних систем та ЗІ СБУ.*

*2010-09-15*

*Практика №1 (3 мала бимсь бути)*

**Інформація** – відомості про об’єкти та явища навколишнього середовища, їхні параметри, властивості та стани, які зменшують наявну про них ступінь невизначеності чи неповноту знань

**Дані** можуть розглядатись як ознаки або записані спостереження, які з будь-яких причин не використовуються, а лише запам’ятовуються(?). У випадку, якщо з’являється можливість використати ці дані для зменшення невизначеності будь-чого, тоді дані перетворюються у інформацію.

При роботі з інформацією завжди є її *джерело* і *споживач*. Шляхи і процеси, що забезпечують передавання повідомлень від джерела інформації до її споживача називається **інформаційними комунікаціями**.

**Адекватність інформації** – це певний рівень відповідності образу, що створюється за допомогою одержаної інформації реального об’єкту, процесу чи явищу. В житті навряд чи можна розраховувати на повну адекватність інформації, оскільки завжди присутня певна ступінь невизначеності. Від ступеня адекватності інформації до реального стану об’єкта або процесу залежить правильність прийняття рішень людини. Адекватність інформації може виражатись у трьох формах: *синтаксичній, семантичній* та *прагматичній*.

**Синтаксична адекватність** відображає формальні структурні характеристики інформації і не зачепає її смислового змісту. На синтаксичному рівні враховується тип носія, спосіб передавання інформації, швидкість передавання і обробку, розміри кодів представлення інформації, надійність і точність перетворення цих кодів та інше.

Інформацію, що розглядають тільки з синтаксичних позицій звичайно називають *даними*, оскільки при цьому немає значення її смислова сторона.

**Семантична (смислова) адекватність** визначає ступінь відповідності опису об’єкта і самого об’єкта та передбачає врахування смислового змісту інформації. Ця форма служить для формування понять та уявлень, виявлення суті, змісту інформації та її узагальнення.

**Прагматична (споживацька) адекватність** відображає відносини інформації та її споживача, відповідність інформації меті управління, яка реалізується на її основі. Ця форма адекватності безпосередньо пов’язана з практичним використанням інформації, з відповідністю її цільової функції діяльності системи.

## Міри інформації

Для вимірювання інформації вводяться два поняття: *кількість інформації* та *об’єм даних*. Ці параметри мають різні вирази та інтерпретацію, залежно від форм адекватності. Для синтаксичної міри інформації міра кількості інформації оперує із знеособленою інформацією, яка не виражає смислового відношення до об’єкту. Об’єм даних ($V\_{д}$) у повідомлені вимірюється кількістю символів(розрядів) у цьому повідомленні. У різних системах числення один розряд має різну вагу і відповідно міняється одиниця вимірювання даних. У двійковій системі числення це – біт, у десятковій – діт. Кількість інформації(I) на синтаксичному рівні неможливо визначити без розміру поняття невизначеності стану системи(ентропія).

Нехай до одержання деякої інформації користувач має попереднє(**апріорні**) відомості про систему $α$. Мірою його необізнаності є функція $H\left(α\right)$, яка в той же час служить і мірою невизначеності стану системи. Після одержання деякого повідомлення $β$ одержувач здобув додаткову інформацію $I\_{β}\left(α\right)$, що зменшила його апріорну необізнаність так, що **апостеріорна**(після одержання повідомлення $β$) стала рівною $H\_{β}\left(α\right)$. Тоді кількість інформації $I\_{β}\left(α\right)$ про систему, одержаної в повідомленні $β$ визначається згідно формули:

$$I\_{β}\left(α\right)=H\left(α\right)-H\_{β}\left(α\right)$$

Тобто кількість інформації вимірюється мірою невизначеності стану системи. Якщо кінцева невизначеність $H\_{β}\left(α\right)$ стане рівною 0, то первинне неповне знання заміниться повним і кількість інформації: $I\_{β}\left(α\right)=H\left(α\right)$. Іншими словами ентропія системи може розглядатись як міра відсутності інформації. Ентропія системи $H(α)$, що має N можливих станів відповідно до формули Шенона обчислюється:

$$H\left(α\right)=-\sum\_{i=1}^{N}p\_{i}log\_{2}p\_{i}$$

*де* $p\_{i}$ *–* ймовірність того, що система знаходиться в i-тому стані. У випадку, якщо всі стани системи є рівно ймовірними, тобто $p\_{i}=\frac{1}{N}$, тоді ентропія визначається так:

$$H\left(α\right)=-\sum\_{i=1}^{N}\frac{1}{N}log\_{2}\frac{1}{N}$$

Досить часто інформація кодується числовими кодами у тій чи іншій системі числення. Особливо це актуально при передачі інформації в ПК. Одна й та ж кількість розрядів у різних системах числення може передавати різне число станів відображуваного об’єкта, що можна представити у вигляді такого співвідношення: $N=m^{n}$, де N – це кількість можливих станів, m – це основа системи числення(різноманіття символів, що застосовується в алфавіті), n – число розрядів у повідомленні.

**Коефіцієнт**(ступінь) **інформативності**(лаконічність) **повідомлення** визначається відношенням кількості інформації до об’єму даних $Y=\frac{I}{V\_{д}}$, при чому $0<Y<1$. Із збільшенням Y зменшується об’єми роботи з перетворення інформації(даних) у системі, тому прагнуть до підвищення інформативності, для чого розробляються спец. методи оптимального кодування інформації.

Для вимірювання смислового змісту інформації, тобто її кількості на семантичному рівні, найбільше визнання одержала *Тезарусна міра*, яка зв’язує семантичні властивості інформації із здатністю користувача сприймати повідомлення що надійшли. **Тезарус** – це сукупність відомостей, якими володіє користувач або система. Залежно від співвідношення між смисловим змістом інформації $S$ і тезаурусом $S\_{p}$ змінюється кількість *семантичної інформації* ($I\_{c}$), що сприймається користувачем і включається ним в подальшому у свій тезаурус. Максимальну кількість семантичної інформації користувач здобуває при узгодженні її смислового змісту S зі своїм тезаурусом Sp, тобто коли інформація, що надходить, є зрозумілою користувачеві, і несе йому раніше невідомі відсутні у його тезарусі відомості. Таким чином кількість семантичної інформації у повідомленні(тобто кількість нових знань, одержаних користувачем) є величиною відносною. Одне і те ж повідомлення може мати смисловий зміст для компетентного користувача і бути безглуздим(семантичний шум) для некомпетентного.

При оцінюванні семантичного спектру інформації необхідно прагнути до узгодження величин S і Sp. Відносною мірою кількості семантичної інформації може правити коефіцієнт змістовності C, який визначається як відношення кількості семантичної інформації до її об’єму.

$$C=I\_{c}/V\_{д}$$

*Лекція*

*2010-09-21*

*Ємець прихворів*

# Основи побудови КС санкціонованого доступу

Механізми, що забезпечують контроль є подібними з іншими механізмами ІБ, а саме: субєкт для доступу до обє'кта, повинен бути однозначно ідентифікований, автентифікований та авторизований. Людські дії можуть бути розподілені в часі і проконтрольовані людьми у режимі близького до реального часу аж до прибуття СБ до місця події в момент злочину

Сучасні системи контролю фізичного доступу як правило мають:

1. Система охорони периметру

2. Контролю та керування доступ

3. Охорона і сигналізація

4. Збереження

Якщо бюджет дозволяє, то ці системи можна інтегрувати в єдину систему - систему керування будівлею, призначенням якої буде не лише контроль доступом, а й облік всіх подій та реєстрацію переміщення авторизованих осіб

Роботи по впровадженню АССД є складними тому повинні виконуватися лише спецами

## Основні терміни

Найбільш важливі терміни з ІБ у світовій практиці та які стосуються систем СД:

**Автоматизована система** - це система, що об'єднує обчислювальну систему, фізичне середовище, персонал, інформацію, що обробляється

**Безпека інформації** - це стан інформації, при якому виключається можливість ознайомлення з інформацією. Ознайомлення з даною інформацією, її модифікація чи знищення корист., які не мають певних повноважень, за рахунок ЕМ наведень, спецзасобів перехоплення чи знищення при передачі цієї і.

Безпека продукції - відсутність недопустимого ризику, пов'язаного з можливістю нанесення збитків

Власник - особа чи організація, яка відповідає за певні інф. ресурсів та за реалізацію необх засобів захисту

ЗІ - сукупність захисту, направлений на забезпечення цілісності І а також доступність І, для користувачів, які мають відповідні повноваження

Комерційна таємниця - відомості конфіденційного хру, розголошення яких може нанести матеріальний чи моральний збиток її власникам чи користувачам

Організація - група людей, які спільно відповідають за виконання робіт та обов'язків

Мета ЗІ: зведення до мінімуму втрат у керуванні, які м.б. викликані порушенням цілісності даних, їх конфіденційності або недоступності інформації, для користувачів і-або процесів, які мають на це відповідні повноваження.

Цінність - властивість І-ї, яка х-зує можливі збитки власника, в наслідок отримання цієї І конкурентами

Уразливість - це можливість виявлення х-рної особливості та недоліків об'єкта захисту, які можуть полегшити проникнення зл. до ресурсів АС

Конфіденційна І - це І-я, яка являє собою комерційну або особисту таємницю та охороняється власником

Нетаємна - не є державною, службовою чи комерційною, особистою таємницею, яка м.б. опублікована у вільному друці.

Загрози І-ї - це потенційно несприятливі впливи на І-ю, які приводять до порушення фундаментальних властивостей захищеної І-ї

Ефективність - степінь досягнутого рівня захищеності ін-ї поставленій меті

Система - комплекс ОТЗ, спрямованих на виявлення, підбиття та ліквідації загроз б.я. виду.

Об'єкт - це сукупність будівель чи приміщень, з розміщеними у них ТЗ обробки, передачі І, об'єднана єдиними інформаційними потоками

Одинарний об'єкт захисту - конкретний носій І-ї, що являє собою єдине ціле та призначений до виконання визначених ф-й. До них відносять людей, що володіють секретами, технічні засоби обробки І, виділені будівлі та приміщення, а також допоміжні ТЗ та системи, які піддаються впливу І фізичних полів

Груповий об'єкт захисту - це структурне об'єднання одинарних об'єктів, які потребують захисту, а також і таких, що не потребують призначених для сумісного виконання визначених функцій

Режимне підприємство - це ГрОбЗахисту, який являє собою підприємство, І-ю про діяльність якого потребують З. від технічних розладів

Охоронна зона об'єкту - це територія, на якій приймаються міри попередженню, проникненню на об'єкт порушників, які здатні спричинити шкоду АС

Рубежі захисту - ств. на об'єкті за допомогою правових, організаційних та техзасобів процедури які попереджують НСД

Засоби контролю керуванням доступом - це механічні, ел-мех, електричні, електронні пристрої, конструкції та ПЗасоби, які забезпечують реалізацію контролю доступом

Доступ - переміщення осіб, транспорту чи інших об'єктів в/з приміщення, зони, території

Розмежування доступу - це порядок використання ресурсів системи при якому суб'єкти отримують доступ до об'єктів у строгій відповідності до правил

Рівень доступу - сукупність часових інтервалів доступу(вікон часу та точок) які призначаються визначеній особі або групі осіб, що мають доступ заданої точки доступу в задані часові інтервали

Точка доступу - місце де безпосередньо здійснюється контроль доступу

Зона доступу - це сукупність точок доступу, пов'язаних спілб