Тема 1-2. Поняття захисту інформації та інформаційної безпеки. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації.

Загроза інформації та можливості прихованої її передачі.

Основні ознаки інформації, що має бути захищеною:

- ✓ наявність певного кола законних власників, що мають право користуватись цією інформацією;
- ✓ наявність зловмисників, що прагнуть оволодіти цією інформацією з корисливою метою для себе та на шкоду законним власникам.

Мета, яку прагнуть досягти зловмисники, називається загрозою. Основні види загроз такі:

- ✓ загроза розголошення конфіденційної (секретної) інформації;
- ✓ загроза цілісності (автентичності, істинності) інформації;
- ✓ загроза достовірності адресних ознак інформації.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Інформація, що є державною власністю, теж вважається конфіденційною.

Цілісність інформації – це відсутність спотворених, замінених або знищених інформаційних елементів.

Достовірність адресних ознак інформації означає відсутність фальсифікації її відправника або отримувача. Це виключає можливість відмовитись від фактів передачі або отримання інформації, якщо вона дійсно передавалась або отримувалась, а також можливість підтвердити передачу або отримання інформації, якщо вона насправді не передавалась і не отримувалась.

Щоб захиститись від загроз, можна скористуватись однієї з трьох можливостей передачі прихованої інформації:

- ✓ використання абсолютно надійного, недоступного для інших каналу зв'язку між абонентами; ця можливість вважається практично нереальною, оскільки, на сучасному рівні науки і техніки неможливо створити такий канал між віддаленими абонентами для неодноразової передачі великих обсягів інформації;
- ✓ використання загальнодоступного каналу зв'язку, але при цьому приховується сам факт передачі інформації; розробкою відповідних методів та засобів займається стенографія;

використання загальнодоступного каналу зв'язку, але при цьому до інформації, що передається, застосовується таке перетворення, що зрозуміти її може тільки адресат; розробкою відповідних методів та способів перетворення інформації займається криптології.

Захист інформації (англ. Data protection) — сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. Термін вживається в Україні для опису комплексу заходів по забезпеченню інформаційної безпеки.

Інформаційна безпека (information security) — збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність.

Конфіденційність (англ. confidentiality, privacy) — властивість не підлягати розголосові; довірливість, секретність, суто приватність.

Типологія конфіденційності

Конфіденційність адміністративна [mandatory confidentiality] — послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом адміністративного.

Конфіденційність довірча [discretionary confidentiality] — послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом довірчого.

Конфіденційність інформації [information confidentiality] — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом.

Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Цілісність (англ. integrity) — внутрішня єдність, пов'язаність усіх частин чого-небудь, єдине ціле. В інформаційній системі — стан даних або інформаційної системи, в якій дані та програми використовуються встановленим чином, що забезпечує:

- стійку роботу системи;
- автоматичне відновлення у випадку виявлення системою потенційної помилки;
- автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи і таке інше.

Цілісність даних [data integrity] — в інформаційній системі — стан при якому дані, що зберігаються в системі, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Цілісність даних вважається збереженою, якщо дані не спотворені і не зруйновані (стерті).

Семантична цілісність даних [semantic data integrity] — стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Цілісність інформації [information integrity] — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або процесом). Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Цілісність бази даних [database integrity] — стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної не суперечливості. Підтримка цілісності бази даних включає перевірку цілісності і відновлення з будь-якого неправильного стану, який може бути виявлено; це входить у функції адміністратора бази даних.

Цілісність системи [system integrity] — властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Цілісність адміністративна [mandatory integrity] — послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів адміністративного керування доступом.

Цілісність довірча [discretionary integrity] — послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів керування доступом довірчого.

Цілісність об'єкта [object integrity] — властивість об'єкта доступу, що характеризує його авторизований стан.

Доступність (англ. Availability) — властивість інформаційного ресурсу, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.

Суть властивості полягає в тому, що потрібний інформаційний ресурс знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Апелювання (англ. non-repudiation) — можливість довести, що автором є саме заявлена людина (юридична особа), і ніхто інший.

Підзвітність (англ. accountability) — властивість інформаційної системи, що дозволяє фіксувати діяльність користувачів, використання ними пасивних об‘єктів та однозначно встановлювати авторів певних дій в системі.

Достовірність (англ. reliability)- властивість інформації, яка визначає ступінь об'єктивного, точного відображення подій, фактів, що мали місце.

Автентичність (англ. authenticity) — властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим.

Відповідно до властивостей інформації, виділяють такі загрози її безпеці:

- ***загрози цілісності:***
  - знищення;

- модифікація;
- ***загрози доступності:***
  - блокування;
  - знищення;
- ***загрози конфіденційності:***
  - несанкціонований доступ (НСД);
  - витік;
  - розголошення.

Аспекти захисту інформації

- ***Конфіденційність*** — захист від несанкціонованого ознайомлення з інформацією.
- ***Цілісність*** — захист інформації від несанкціонованої модифікації.
- ***Доступність*** — захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

Кожен вид ЗІ забезпечує окремі аспекти ІБ:

Технічний — забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, токіни, смарт-карти тощо):

- попередження витоку по технічним каналам;
- попередження блокування;

Інженерний — попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація).

Криптографічний — попереджує доступ до за допомогою математичних перетворень повідомлення:

- попередження несанкціонованої модифікації ;
- попередження НС розголошення.

Організаційний — попередження доступу на об’єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу).

Інформаційні системи можна розділити на три частини: *програмне забезпечення*, *апаратне забезпечення* та *комунікації* з метою цільового застосування (як механізму захисту і попередження) стандартів інформаційної безпеки. Самі механізми захисту реалізуються на трьох рівнях або шарах: Фізичний, Особистісний, Організаційний. По суті, реалізація політик і процедур безпеки покликана надавати інформацію адміністраторам, користувачам і операторам про те як правильно використовувати готові рішення для підтримки безпеки.

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завданий збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між всіма елементами соціуму.

Враховуючи вплив на трансформацію ідей інформаційної безпеки, в розвитку засобів інформаційних комунікацій можна виділити декілька етапів:

I етап — до 1816 року — характеризується використанням природно виникаючих засобів інформаційних комунікацій. В цей період основне завдання інформаційної безпеки полягало в захисті відомостей про події, факти, майно, місцезнаходження і інші дані, що мають для людини особисто або співтовариства, до якого вона належала, життєве значення.

II етап — починаючи з 1816 року — пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Для забезпечення скритності і перешкодостійкості радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на вищому технологічному рівні, а саме застосування перешкодостійкого кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу).

III етап — починаючи з 1935 року — пов'язаний з появою засобів радіолокацій і гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційних і технічних заходів, направлених на підвищення захищеності засобів радіолокацій від дії на їхні приймальні пристрої активними маскуючими і пасивними імітуючими радіоелектронними перешкодами.

IV етап — починаючи з 1946 року — пов'язаний з винаходом і впровадженням в практичну діяльність електронно-обчислювальних машин (комп'ютерів). Завдання інформаційної безпеки вирішувалися, в основному, методами і способами обмеження фізичного доступу до устаткування засобів добування, переробки і передачі інформації.

V етап — починаючи з 1965 року — обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, в основному, методами і способами фізичного захисту засобів добування, переробки і передачі інформації, об'єднаних в локальну мережу шляхом адміністрування і управління доступом до мережевих ресурсів.

VI етап — починаючи з 1973 року — пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. Загрози інформаційній безпеці стали набагато серйознішими. Для забезпечення інформаційної безпеки в комп'ютерних системах з безпровідними мережами передачі даних потрібно було розробити нові критерії безпеки. Утворилися співтовариства людей — хакерів, що ставлять собі за мету нанесення збитку інформаційній безпеці окремих користувачів, організацій і цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а забезпечення його безпеки — найважливішою і обов'язковою складовою національної безпеки. Формується інформаційне право — нова галузь міжнародної правової системи.

VII етап — починаючи з 1985 року — пов'язаний із створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Можна припустити що черговий етап розвитку інформаційної безпеки, очевидно, буде пов'язаний з широким використанням надмобільних комунікаційних пристроїв з широким спектром завдань і глобальним охопленням у просторі та часі, забезпечуваним космічними інформаційно-комунікаційними системами. Для вирішення завдань інформаційної безпеки на цьому етапі необхідним є створення макросистеми інформаційної безпеки людства під егідою ведучих міжнародних форумів.

Базові поняття інформаційної безпеки:

Інформаційна безпека держави — 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.

Інформаційна безпека організації — цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Інформаційна безпеки особистості характеризується як стан захищеності особистості, різноманітних соціальних груп та об'єднань людей від впливів, здатних проти їхньої волі та бажання змінювати психічні стани і психологічні характеристики людини, модифікувати її поведінку та обмежувати свободу вибору.

Забезпечення ІБ держави

Згідно з українським законодавством, вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;

- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Забезпечення ІБ підприємства/організації

В Україні забезпечення ІБ здійснюється шляхом захисту інформації — у випадку, коли необхідність захисту інформації визначена законодавством в галузі ЗІ. Для реалізації захисту інформації створюється Комплексна система захисту інформації (КСЗІ), або, у випадку, коли суб'єкт ІБ має наміри розробити і реалізувати політику ІБ і може реалізовувати їх без порушення вимог законодавства:

- міжнародними стандартами ISO: ISO/IEC 17799:2005, ISO/IEC 27001:2005 та ін. — для підтримки рішень на основі ITIL та COBIT і виконання вимог англ. Sarbanes-Oxley Act (акту Сербайнза-Оклі про відповідальність акціонерів за обізнаність про стан своїх активів). Тоді на підприємстві створюється Система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі ІБ.
- власними розробками.

Забезпечення ІБ особистості

Органи (підрозділи) забезпечення ІБ

1. Міжнародні організації
2. Державні органи

- Відділи спецслужб держави. Спеціально уповноважений орган держави з питань захисту інформації (зараз в Україні —це Державна служба спеціального зв'язку та захисту інформації (скор. ДССЗЗІ)

3. Підрозділи підприємства

На підприємстві функцію забезпечення ІБ може виконувати як окремий відділ Служби безпеки підприємства, так і окрема Служба (Служба захисту інформації).

Для контролю за КСЗІ в обов'язковому порядку створюється Служба захисту інформації в інформаційно-телекомунікаційній системі (сама назва «Служба» не є обов'язковою).

Функції з контролю за СУІБ покладаються на певний відділ підприємства.

Законодавчі вимоги і регулювання ІБ

Загальнозаконодавчі вимоги – інформаційне законодавство держави, спеціалізовані нормативні акти (в Україні — це Нормативні документи в галузі технічного захисту інформації (скор. НД ТЗІ).

Галузеві вимоги (галузеві стандарти тощо).

Критерії оцінки інформаційної безпеки (англ. Common Criteria) є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

За допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Для характеристики основних критеріїв інформаційної безпеки застосовують модель тріади CIA.

Ця система передбачає такі основні характеристики інформаційної безпеки як конфіденційність, цілісність, доступність.

Інформаційні системи аналізуються в трьох головних секторах: технічних засобах, програмному забезпеченні і комунікаціях, з метою ідентифікування і застосування промислових стандартів інформаційної безпеки, як механізми захисту і запобігання, на трьох рівнях або шарах: фізичний, особистий і організаційний. По суті, процедури або правила запроваджуються для інформування адміністраторів, користувачів та операторів щодо використовування захисної продукції для гарантування інформаційної безпеки в межах організацій.

В Україні також розробляються і використовуються критерії інформаційної безпеки. Наприклад

департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України прийняв нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» який подібний до моделі тріади CIA.

Функціональні критерії

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги відносяться до критеріїв конфіденційності.

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. У випадку, якщо існують вимоги щодо обмеження можливості модифікації інформації, то їх відносяться до критеріїв цілісності.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то їх відносяться до критеріїв доступності.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні функції відносяться до критеріїв спостереженості.

Окрім функціональних критеріїв захищеності існують таки критерії гарантій, що дозволяють оцінити коректність реалізації систем захисту. Ці критерії включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається інформаційною безпекою?
2. Дайте визначення поняття захисту інформації.
3. Назвіть та охарактеризуйте основні властивості інформації.
4. Назвіть та охарактеризуйте основні аспекти захисту інформації та інформаційної безпеки.
5. Які виділяють загрози безпеки інформації відповідно до її властивостей?
6. Назвіть та дайте визначення базовим поняттям інформаційної безпеки.
7. Охарактеризувати шляхи забезпечення інформаційної безпеки держави, підприємства, особистості.
8. Назвати та охарактеризувати основні критерії інформаційної безпеки.
9. Що являють собою законодавчі вимоги до інформаційної безпеки?
10. Що являє собою модель тріади CIA?