Тема 1. Основні положення інформаційної безпеки

План:

1. **Поняття інформаційної безпеки**
2. **Основні задачі інформаційної безпеки**
3. **Важливість і складність проблем інформаційної безпеки - СРС**
4. **Об’єктно-орієнтований підхід до інформаційної безпеки - СРС**
5. **Основні положення системи захисту інформації**

1. Поняття інформаційної безпеки

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

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

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. (*ЗУ “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки”)*

Інформаційна безпека – 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.

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.

Інформаційна безпека ІС залежить не тільки від комп’ютерів, але й від інфраструктури, що її підтримує, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал.

Найслабша ланка ІБ - людина

У визначені ІБ : « … ***неприйнятні втрати***… »
??????

2. Основні задачі інформаційної безпеки

Успіх ІБ - систематичний, комплексний підхід.

Основні задачі ІБ:

забезпечення доступності інформації;

забезпечення цілісності інформації;

забезпечення конфіденційності інформації;

забезпечення вірогідності інформації;

забезпечення юридичної значимості інформації, представленої у вигляді електронного документа;

забезпечення невідстежуваності дій користувача

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

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

Цілісність буває двох видів:

- *статична* (тобто незмінність інформаційних об’єктів) ;
- *динамічна* (стосується коректного виконання складних дій (транзакцій)

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

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

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

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

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 працездатності ІС **повинна забезпечувати захист від:**

порушення функціонування інформаційної системи шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системного і прикладного програмного 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 засобів захисту, що вбудовуються, і зовнішніх засобів;

неправомірних дій користувачів і обслуговуючого персоналу мережі

Для забезпечення інформаційної безпеки в необхідно:

- захистити інформацію під час її зберігання, оброблення і передавання мережею;
- підтвердити дійсність об’єктів даних і користувачів (автентифікація сторін, що встановлюють зв’язок);
- знайти і попередити порушення цілісності об’єктів даних;
- захистити технічні пристрої і приміщення;
- захистити конфіденційну інформацію від витоку і від вбудованих електронних пристроїв знімання інформації;
- захистити програмні засоби від під’єднання 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 в цілому;
- організувати заходи, що спрямовані на забезпечення збереження конфіденційних даних.

3. Важливість і складність проблеми інформаційної безпеки

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

При аналізі 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. Сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення ІБ.

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.

4. Об’єктно-орієнтований підхід до інформаційної безпеки

Об’єктно-орієнтований підхід є основою сучасної технології програмування, випробуваним методом боротьби зі складністю систем. В ІБ не віддзеркалився.

Метод боротьби зі складністю спирається на принцип “Divide et impera” – “розділяй і володарюй”

Грані ІБ в контексті **об’єктно-орієнтованого підходу**

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

Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки.

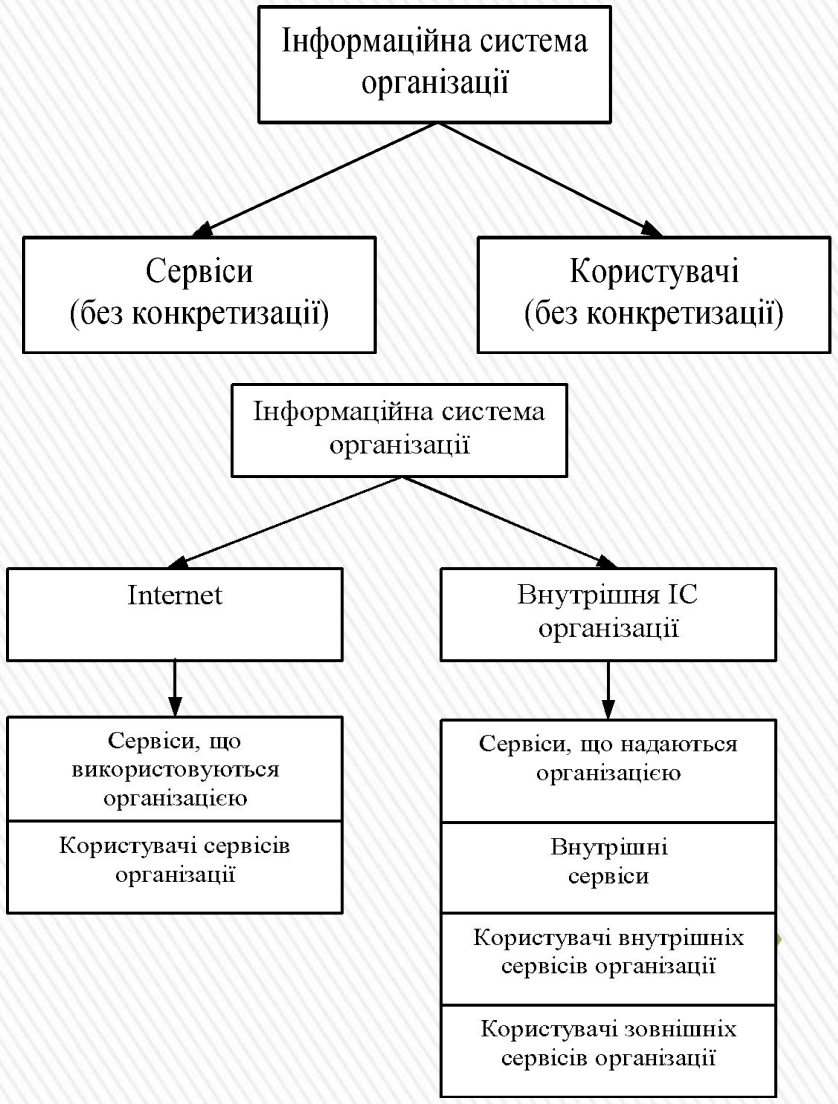
Системи ІБ є досить складними, що потребують деталізації.

Поняття *рівня деталізації* важливе для систематичного розгляду складних систем, представлених 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.

Рівні деталізації

Нульовий рівень деталізації. Йому відповідає інформаційна система в цілому. Необхідно врахувати закони, застосовні до організацій, що мають в своєму розпорядженні інформаційні системи.

На першому рівні деталізації визначаються сервіси і користувачі, або, інакше кажучи, здійснюється поділ на клієнтську і серверну частину



На другому рівні деталізації ще не описується внутрішня структура ІС організації і деталі Internet. Констатується тільки існування зв’язку між цими мережами, наявність в них користувачів, а також внутрішніх та зовнішніх сервісів без опису їхнього змісту

5. Основні положення системи захисту інформації

Система захисту інформації – це організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

Безпека інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту в усіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації

Система захисту інформації – єдиний цілісний механізм методів, засобів та заходів щодо ІБ, що повинен контролюватися, оновлюватися і доповнюватися.

Захист інформації повинен бути (вимоги):

- **неперервним**. Ця вимога виникає з того, що зловмисники тільки і шукають можливість, як би обійти захист інформації, що цікавить їх;
- **плановим**. Планування здійснюється шляхом розробки кожною службою детальних планів захисту інформації у сфері її компетенції з урахуванням загальної мети підприємства (організації);
- **цілеспрямованим**. Захищається тільки те, що повинно захищатися в інтересах конкретної мети, а не все підряд;
- **конкретним**. Захисту підлягають конкретні дані, що об’єктивно вимагають охорони, втрата яких може заподіяти організації певний

Захист інформації повинен бути (продовження) :

- **універсальним**. Вважається, що залежно від виду каналу витоку або способу несанкціонованого доступу його необхідно перекривати, де б він не проявився, розумними і достатніми засобами, незалежно від характеру, форми і виду інформації;

- **комплексним**. Для захисту інформації повинні застосовуватися всі види і форми захисту в повному обсязі. Неприпустимо застосовувати лише окремі форми чи технічні засоби. Комплексний характер захисту виникає з того, що захист – це специфічне явище, що є складною системою нерозривно взаємопов’язаних і взаємозалежних процесів, кожний з яких, у свою чергу, має безліч різних сторін, властивостей, тенденцій.

Система захисту інформації повинна задовольняти такі умови:

охоплювати весь технологічний комплекс інформаційної діяльності;

бути різноманітною за використовуваними засобами, багаторівневою з ієрархічною послідовністю доступу;

бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;

бути нестандартною, різноманітною. Вибираючи засоби захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей;

бути простою для технічного обслуговування і зручною для експлуатації користувачами;

бути надійною. Будь-які несправності технічних засобів є причиною появи неконтрольованих каналів витоку інформації;

бути комплексною, мати цілісність, що означає, що жодна її частина не може бути вилучена без втрат для всієї системи.

До системи безпеки інформації висуваються також певні вимоги:

чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;

надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;

зведення до мінімуму кількості спільних для декількох користувачів засобів захисту;

облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;

забезпечення оцінювання ступеня конфіденційної інформації;

забезпечення контролю цілісності засобів захисту і негайне реагування на вихід їх з ладу.

Види забезпечення СЗІ

- **правове забезпечення**. Сюди входять нормативні документи, положення, інструкції, посібники, вимоги яких є обов'язковими в рамках сфери їх дій;
- **організаційне забезпечення**. Мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями – такими, як служба захисту документів; служба режиму, допуску, охорони; служба захисту інформації технічними засобами; інформаційно-аналітична діяльність і ін.;
- **апаратне забезпечення**. Передбачається широке використання технічних засобів як для захисту інформації, так і для забезпечення діяльності власне СЗІ;
- **інформаційне забезпечення**. Воно містить у собі відомості, дані, показники, параметри, які лежать в основі розв’язання задач, що забезпечують функціонування системи. Сюди можуть входити як показники обліку, зберігання, так і системи інформаційного забезпечення розрахункових задач різного характеру, пов’язаних з діяльністю служби забезпечення безпеки;

Види забезпечення СЗІ

- **програмне забезпечення**. До нього належать різні інформаційні, облікові, статистичні і розрахункові програми, що забезпечують оцінювання наявності і небезпеки різних каналів витоку і шляхів несанкціонованого проникнення до джерел конфіденційної інформації;
- **математичне забезпечення**. Припускає використання математичних методів для різних розрахунків, пов'язаних з оцінюванням небезпеки технічних засобів зловмисників, зон і норм необхідного захисту;
- **лінгвістичне забезпечення**. Сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері захисту інформації;
- **нормативно-методичне забезпечення**. Сюди входять норми і регламенти діяльності органів, служб, засобів, які реалізують функції захисту інформації, різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації

Задовольнити сучасні вимоги до забезпечення безпеки підприємства може тільки система безпеки

Як і будь-яка система, інформаційної безпеки має свої мету, задачі, методи і засоби діяльності, що узгоджуються за місцем і часом, залежно від умов.

Система безпеки – це організована сукупність спеціальних установ, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз.

» Дякую за увагу!!!