ТЕМА 1.
СУТНІСТЬ ТА ОСНОВНІ ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Питання лекції:

1. Про концепцію інформаційної безпеки України.
2. Основні задачі інформаційної безпеки.
3. Джерела загроз інформаційній безпеці.
4. Методи запобігання та ліквідації загроз інформаційній безпеці.
5. Організаційні основи захисту інформації.
6. Організаційно-технічні заходи щодо ТЗІ на об’єкті.

Література:

- Закон України "Про інформацію";
- Закон України "Про захист інформації в автоматизованих системах";
- Закон України "Про науково-технічну інформацію";
- Закон України "Про державну таємницю";
- Концепція (основи державної політики) національної безпеки України;
- Концепція технічного захисту інформації в Україні;
- Положення про порядок здійснення криптографічного захисту інформації в Україні;
- НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах

від несанкціонованого доступу.

1. Базові терміни та визначення

Інформаційний простір — середовище, де здійснюється формування, збір, зберігання та розповсюдження інформації.

Інформаційний ресурс — це складова інформаційного простору, що поєднує в собі дані, їх місцезнаходження, взаємозв’язок між інформаційними елементами, відомості (про процеси надходження, зберігання, обробки тощо).

Інформаційна інфраструктура — це складова інформаційного простору, яка являє собою сукупність даних (структурованих чи неструктурованих); засобів збору, накопичення, обробки, збереження та розповсюдження інформації; системи виробництва інформаційних продуктів; інформаційних ресурсів зовнішнього інформаційного простору; інструктивних матеріалів та документації; людини як активного фактору вплину на інформаційний простір.

Інформаційна безпека — стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави.

Об'єкт інформаційної безпеки. Соціальними об'єктами інформаційної безпеки є: особа — її права та свободи в інформаційній сфері; суспільство — його духовні цінності, засади солідарної діяльності; держава — її конституційний лад, суверенітет, ефективне функціонування. Технічними об'єктами інформаційної безпеки є інформаційні ресурси, інформаційна інфраструктура, інформаційні технології.

Загрози інформаційній безпеці — фактор або їх сукупність, що створюють небезпеку функціонуванню та розвитку інформаційного простору, інтересам особистості, суспільства, держави.

Захист інформації — сукупність засобів, методів, організаційних заходів щодо попередження можливих випадкових або навмисних впливів природного чи штучного характеру, наслідком яких може бути нанесення збитків чи шкоди власникам інформації або її користувачам, інформаційному простору. Суттю захисту інформації є її доступність при збереженні цілісності інформації та гарантованій конфіденційності.

Інформаційна безпека відіграє суттєву роль в забезпеченні життєво важливих інтересів будь-якої країни. Метою забезпечення інформаційної безпеки в Україні є створення розгалуженого та захищеного інформаційного

простору, захист національних інтересів України в умовах формування світових інформаційних мереж, захист економічного потенціалу держави від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ та держави на отримання, поширення та використання інформації.

2. Основні задачі забезпечення інформаційної безпеки:

• виявлення, оцінка та прогнозування джерел загроз інформаційній безпеці;

• розробка державної політики забезпечення інформаційної безпеки та комплексу заходів і механізмів її реалізації;

• створення нормативно-правових засад забезпечення інформаційної безпеки, координація діяльності органів державної влади та управління, установ та підприємств по реалізації політики інформаційної безпеки;

• розвиток системи забезпечення інформаційної безпеки, вдосконалення її організації, форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідації наслідків її порушення;

• забезпечення участі в процесах створення і використання глобальних інформаційних мереж та систем.

3. Джерела загроз інформаційній безпеці

До джерел загроз належать:

• недружня політика іноземних держав в галузі глобального інформаційного моніторингу, поширення інформації та новітніх інформаційних технологій;

• цілеспрямована діяльність іноземних спецслужб, політичних та економічних структур;

• злочинна діяльність міжнародних угрупувань, формувань та окремих осіб;

• неправомірна чи протиправна діяльність посадових осіб державних органів, структур, формувань, спрямована проти інтересів України;

• стихійні лиха, катастрофи, збройні конфлікти;

• недосконаліть технічних і програмних засобів та недостатня кваліфікація персоналу інформаційних служб і систем;

• недосконаліть, неповнота і неузгодженість з відповідними міжнародними правовими актами чинного законодавства України в інформаційній сфері;

• недостатній розвиток лексикографічної бази української мови і національного лінгвістичного забезпечення інформаційних систем;

• низькі темпи науково-технічного і культурного розвитку суспільства внаслідок економічної кризи або неадекватної внутрішньої політики держави в інформаційній сфері;

• низька правова, організаційна та програмно-технічна забезпеченість в галузі інформаційної безпеки.

Засоби впливу загроз на інформаційну безпеку поділяються на інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-правові.

До інформаційних засобів належать:

• порушення адреси і своєчасності інформаційного обміну, протизаконні збір і використання інформації;

• несанкціонований доступ до інформаційних ресурсів;

• маніпулювання інформацією (дезінформація, укриття та викривлення інформації);

• незаконне копіювання інформації в інформаційних системах;

• використання засобів масової інформації з позицій, які суперечать інтересам громадян, організацій чи держави;

• викрадення інформації з бібліотек, архівів, банків і баз даних;

• порушення технології обробки інформації.

До програмно-математичних засобів належать: запуск програм-вірусів; установка програмних і апаратних закладних пристроїв; знищення і модифікація даних в інформаційних системах.

Фізичні засоби включають:

• знищення або руйнування засобів обробки інформації і зв’язку; знищення, руйнування чи викрадення оригінальних носіїв інформації;

• викрадення програмних чи апаратних ключів і засобів криптографічного захисту інформації; вплив на персонал;

• поставка ―інфікованих компонентів інформаційних систем.

До радіоелектронних засобів належать:

• перехоплення інформації в технічних каналах її витоку;

• будова електронних пристроїв перехоплення інформації в технічних засобах і приміщеннях;

• перехоплення, дешифрування та подання хибної інформації в мережах передачі даних і мережах зв’язку;

• вплив на парольно-ключові системи;

• радіоелектронне придушення мереж зв’язку і систем керування.

До організаційно-правових засобів належать:

• купівля недосконалих або застарілих інформаційних технологій та засобів інформатизації; невиконання вимог законодавства та затримку прийняття необхідних нормативно-правових положень в інформаційній сфері;

• неправомірне обмеження доступу, до документів, в яких знаходиться важлива для громадян та організацій інформація.

Реалізація інформаційних загроз на рівні особи призводить до порушення або обмеження доступу громадян до інформації загального користування. Це створює загрозу інформаційній безпеці особистості як з боку органів влади, так і з боку сторонніх осіб або угрупувань, порушує баланс стосунків між особистістю, суспільством і державою. :

Наслідком впливу інформаційних загроз на соціальну спільноту є ускладнення соціальних процесів, що виявляється у загостренні суперечностей між різними соціальними прошарками, загостренні політичної боротьби, розпалюванні релігійних та етнічних суперечностей, зниженні загальної

культури населення, розвитку бездуховності, зростанні злочинності, розповсюдженні антигуманних ідей.

Наслідки інформаційних злочинів в економічній сфері можуть призвести до економічних втрат за рахунок знецінення і втрати товарної частини інформаційного ресурсу — промислових і інформаційних технологій.

4. Методи запобігання та ліквідації загроз інформаційній безпеці

Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмно-технічні і організаційно-економічні методи.

Правові методи - передбачають розробку комплексу нормативно-правових актів і положень, регламентуючих інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки.

Програмно-технічні методи — це сукупність засобів:

• запобігання витоку інформації,

• виключення можливості несанкціонованого доступу до інформації,

• запобігання впливам, які призводять до знищення, руйнування, спотворення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації,

• виявлення закладних пристроїв,

• виключення перехоплення інформації технічними засобами,

• використання криптографічних засобів захисту інформації при передачі по каналах зв’язку.

Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих систем згідно вимогам інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту інформації, контроль за діями персоналу в захищених інформаційних системах.

5. Організаційні основи захисту інформації.

В загальному принципи захисту інформації можна умовно розділити на дві основні групи:

1) правові принципи;

2) організаційні принципи;

Правові принципи захисту інформації

Правове регулювання захисту інформації спирається на принципи інформаційного права. Дані принципи, що базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а так само гарантують їх здійснення. Крім того, основні правові засади захисту інформації ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкту правовідносин.

Узагальнено до правових принципів захисту інформації відносяться: легітимність (законність); пріоритет міжнародного права над внутрішньодержавним; економічна доцільність.

Організаційні принципи захисту даних

Роль організаційного захисту інформації в системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.

Організаційні методи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, а так само включають в себе наступні принципи захисту інформації:

• науковий підхід до організації захисту інформації;

• планування захисту ;

• керування системою захисту;

• безперервність процесу захисту інформації;

• мінімальна достатність організації захисту;

• системний підхід до організації та проектування систем та методів захисту інформації;

• комплексний підхід до організації захисту інформації;

• відповідність рівня захисту цінності інформації;

• гнучкість захисту;

• багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки;

• багаторубіжність захисту інформації;

• обмеження числа осіб, які допускаються до захищеної інформації;

• особиста відповідальність персоналу за збереження довіреної інформації.

6. Організаційно-технічні заходи щодо ТЗІ на об'єкті.

Технічний захід – це дія із захисту інформації, яка передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи включають:

- встановлення за допомогою технічних засобів потенційних каналів витоку інформації та визначення методів та засобів для їх блокування;

- перевірку техніки, яка використовується, на відповідність величини паразитних випромінювань допустимим рівням;

- екранування приміщень або техніки, яка використовується;

- перемонтаж окремих мереж, кабелів та ліній зв'язку;

- застосування спеціальних пристроїв і засобів захисту;

- використання засобів активного захисту;

- перевірку адекватності та надійності функціонування застосованих технічних засобів рівню потенційних загроз.

На початку робіт з ТЗІ необхідно визначити види інформації та від якого роду загроз треба захищатися. Для цього в першу чергу визначають категорію приміщення.

При цьому з'ясовують види та ступень таємності інформації, що може циркулювати у приміщенні. Далі розглядаються конструктивні особливості

приміщення та умови його розташування, наявність побутової техніки та апаратури для обробки інформації, її типи та технічні характеристики. З'ясовується та враховується наявність біля об'єкту, що треба захищати, іноземних установ, автостоянок, приватних фірм (тобто місць, з яких можна організувати стаціонарне та мобільне зняття інформації). Заміряється відстань до таких місць і визначається охоронна зона, в межах якої несанкціоноване зняття інформації вважається неможливим. Це надає змогу з'ясувати типи та ступень можливих загроз та встановити відповідну категорію захисту інформації.

Якщо поряд з об'єктом є іноземні установи чи фірми, де можна організувати стаціонарне зняття інформації, категорійність приміщення підвищується на один ступінь.

Складається акт про встановлення категорійності приміщення, в якому відбиваються всі питання, що перераховані вище. Такий акт складається представниками підрозділу з ТЗІ та членами комісії, яка призначається керівником установи, де проводяться такі роботи.

Встановлення категорійності приміщення надає змогу скласти план робіт з ТЗІ, в якому визначаються обсяги та напрямки проведення робіт з ТЗІ, термін їх проведення, необхідні технічні засоби для захисту інформації на об'єкті. Ці роботи повинен проводити ліцензіант, тобто установа, яка має державну ліцензію на проведення таких робіт. Надалі всі роботи з ТЗІ проводяться ліцензіантом. Якщо в установі є підрозділ з ТЗІ, який має ліцензію на виконання всього потрібного обсягу робіт, то ці роботи можуть проводитися таким підрозділом.

При проведенні робіт з ТЗІ необхідно провести ряд заходів, зокрема:

- визначити та змонтувати необхідні технічні засоби, що потрібні для захисту інформації на об'єкті;

- провести необхідні вимірювання, які б підтвердили ефективність застосування обраних технічних засобів захисту та їх правильне функціонування.

Після проведення всього комплексу технічних робіт ліцензіант разом з замовником складають акт про надання об’єкту певної категорії із захисту інформації.

Лише після одержання та затвердження такого акту на об’єкті можна обробляти інформацію з обмеженим доступом.

Технічний захист інформації від її несанкціонованого зняття полягає в застосуванні спеціальних технічних методів її захисту, які блокують потенційні канали витоку інформації, тобто заважають спробам її незаконного отримання.

Для того, щоб захищати інформацію від витоку необхідно знати потенційні канали витоку та методи їх блокування.