ТЕМА Методи та засоби захисту комп’ютерної інформації.

Інформація як об’єкт захисту

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних від злочинних зазіхань зловмисників.

Концентрація інформації в комп'ютерах (аналогічно концентрації готівки в банках) змушує одних усе більш підсилювати пошуки шляхів доступу до інформації, а інших, відповідно, підсилювати контроль над нею з метою захисту.

Складність створення системи захисту інформації визначається тим, що дані можуть бути викрадені з комп'ютера (скопійовані), одночасно залишаючись на місці. Цінність деяких даних полягає у володінні ними, а не в їх знищенні або зміні.

Забезпечення безпеки інформації – справа дорога, і не стільки через витрати на закупівлю або установку різних технічних або програмних засобів, скільки через те, що важко кваліфіковано визначити межі розумної безпеки і відповідної підтримки системи в працездатному стані.

Об'єктами зазіхань можуть бути як самі матеріальні технічні засоби (комп'ютери і периферія), так і програмне забезпечення і бази даних.

Кожен збій роботи комп'ютерної мережі – це не тільки моральний збиток для працівників підприємства, корпорацій і мережевих адміністраторів. У процесі розвитку технологій електронних платежів, «без паперового» документообігу серйозний збій локальних мереж може паралізувати роботу цілих підприємств, що призведе до відчутних збитків. Не випадково захист даних у комп'ютерних мережах стає однією із найгостріших проблем.

Забезпечення безпеки інформації у комп'ютерних мережах припускає створення перешкод для будь – яких несанкціонованих спроб розкрадання або модифікації даних, що передані у мережі. При цьому дуже важливо зберегти такі властивості інформації, як:

• доступність,

• цілісність,

• конфіденційність.

Доступність інформації – здатність забезпечувати своєчасний і безперешкодний доступ користувачів до інформації, яка їх цікавить.

Цілісність інформації полягає в її існуванні в неспотвореному вигляді (незмінному стосовно деякого фіксованого її стану).

Конфіденційність – це властивість, що вказує на необхідність введення обмежень доступу до даної інформації для визначеного кола користувачів.

Для того, щоб правильно оцінити можливий реальний збиток від втрати інформації, що зберігається на комп'ютері, необхідно знати, які загрози при цьому можуть виникнути і які адекватні заходи для її захисту необхідно приймати.

Характеристика загроз безпеки інформації

Неправомірне перекручування, фальсифікація, знищення або розголошення конфіденційної інформації може нанести серйозні, а іноді й непоправні матеріальні або моральні втрати. У цьому випадку, досить важливим є забезпечення безпеки інформації без збитку для інтересів тих, кому вона призначена.

Щоб забезпечити гарантований захист інформації в комп'ютерних системах обробки даних, потрібно насамперед сформулювати мету захисту інформації і визначити перелік необхідних заходів, які забезпечують захист. Для цього необхідно, в першу чергу, розглянути і систематизувати всі можливі фактори(загрози), що можуть призвести до втрати або перекручування вихідної інформації.

Під **загрозою безпеки комп'ютерної системи** розуміється подія (вплив), що у випадку своєї реалізації стане причиною порушення цілісності інформації, її втрати або заміни. **Загрози можуть** бути як випадковими, так і навмисними.

До випадкових загроз відносять:

1. Помилки обслуговуючого персоналу і користувачів;
2. Втрата інформації, обумовлена неправильним збереженням архівних даних;
3. Випадкове знищення або зміна даних;
4. Збої устаткування і електроживлення;
5. Збої кабельної системи;
6. Перебої електроживлення;
7. Збої дискових систем;
8. Збої систем архівування даних;
9. Збої роботи серверів, робочих станцій, мережевих карт і т.д.;
10. Некоректна робота програмного забезпечення;
11. Зміна даних при помилках у програмному забезпеченні;
12. Зараження системи комп'ютерними вірусами;
13. Несанкціонований доступ;
14. Випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.

Найчастіше збиток спричиняється не через чийсь злий намір, а просто через елементарні помилки користувачів, що випадково псують або видаляють дані, життєво важливі для системи. У зв'язку з цим, крім контролю доступу, необхідним елементом захисту комп’ютерної інформації є розмежування повноважень користувачів.

Крім того, ймовірність помилок обслуговуючого персоналу і користувачів мережі може бути значно зменшена, якщо їх правильно навчати і, періодично контролювати їх дії зі сторони, наприклад, адміністратора мережі.

Надійний засіб запобігання втрат інформації при короткочасному відключенні електроенергії – установка джерел безперебійного живлення (UPS). Різні за своїми технічними і споживчими характеристиками, подібні пристрої можуть забезпечити живлення всієї локальної мережі або окремого комп'ютера упродовж часу, достатнього для відновлення подачі напруги або для збереження інформації на магнітних носіях. Більшість UPS виконують функції ще і стабілізатора напруги, що є додатковим захистом від стрибків напруги в мережі. Багато сучасних мережевих пристроїв (сервери, концентратори і ін.) оснащені власними дубльованими системами електроживлення.

Основний, найбільш розповсюджений, метод захисту інформації і устаткування від стихійних лих (пожеж, землетрусів, повеней.) полягає у створенні та збереженні архівних копій даних.

Особливістю комп'ютерних технологій є те, що безпомилкових програм, у принципі, не буває. Якщо проект, практично у будь – якій галузі техніки, можна виконати із величезним запасом надійності, то в галузі програмування така надійність досить умовна, а іноді майже недосяжна. І це стосується не тільки окремих програм, але і цілого ряду програмних продуктів фірм, відомих в усьому світі.

Через недоліки у програмних продуктах Microsoft, пов'язаних із забезпеченням безпеки даних у мережі Internet, «хакери» можуть захоплювати особисті ключі шифрів користувачів і діяти від їх імені.

Нині більше половини користувачів випробували «на собі » дію вірусів. Найбільш розповсюдженим методом захисту від вірусів дотепер залишається використання різних антивірусних програм.

Рівень зазначених загроз значно знижується за рахунок підвищення кваліфікації обслуговуючого персоналу і користувачів, а також надійності апаратно – програмних і технічних засобів. Однак, найбільш небезпечним джерелом загроз інформації є навмисні дії зловмисників.

Стандартність архітектурних принципів побудови устаткування і програм забезпечує порівняно легкий доступ професіонала до інформації, що знаходиться в персональному комп’ютері. Обмеження доступу до ПК шляхом введення кодів не гарантує стовідсотковий захист інформації.

Включити комп'ютер і зняти код доступу до системи не викликає особливих труднощів: досить відключити акумулятор на материнській платі. На деяких моделях материнських плат для цього передбачений спеціальний перемикач. Також у кожного виробника програми BIOS (AMI, AWARD і ін.) є коди, що мають пріоритет перед будь – якими кодами користувачів, набравши які можна одержати доступ до системи. У крайньому разі, можна вкрасти системний блок комп'ютера або витягти жорсткий диск і вже без перешкод одержати доступ до необхідної інформації.

Загрози, що навмисно створюються зловмисником або групою осіб (навмисні загрози), заслуговують більш детального аналізу, тому що часто носять витончений характер і призводять до важких наслідків. Тому розглянемо їх докладно.

До навмисних загроз відносять:

• несанкціонований доступ до інформації і мережевих ресурсів;

• розкриття і модифікація даних і програм, їх копіювання;

• розкриття, модифікація або підміна трафіка обчислювальної мережі;

• розробка і поширення комп'ютерних вірусів;

• крадіжка магнітних носіїв і розрахункових документів;

• руйнування архівної інформації або навмисне її знищення;

• фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому;

• перехоплення та ознайомлення з інформацією, яка передана по каналах зв'язку тощо.

Виділяють три **основних види загроз безпеки:** загрози розкриття, цілісності і відмови в обслуговуванні (рис. 1.1).

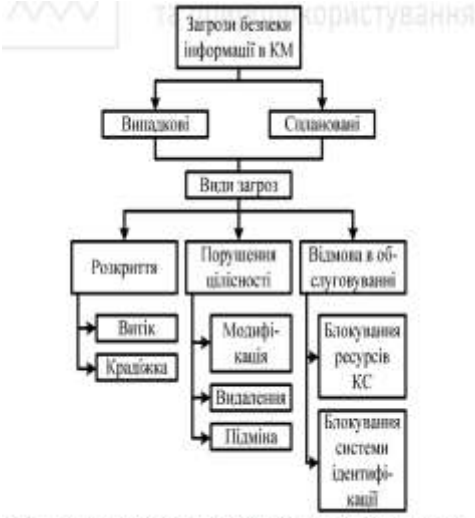

Рис. 1.1 Види загроз безпеки інформації в комп'ютерних мережах

Загроза розкриття полягає в тім, що інформація стає відомою тому, кому не потрібно її знати. Іноді замість слова «розкриття» використовуються терміни «крадіжка» або «витік».

Загроза порушення цілісності – будь – яка навмисна зміна (модифікація або навіть видалення) даних, що зберігаються в обчислювальній системі або передаються з однієї системи в іншу. Звичайно вважається, що загрозі розкриття найбільше піддаються державні структури, а загрозі порушення цілісності – ділові або комерційні.

Загроза відмови в обслуговуванні виникає всякий раз, коли у результаті певних дій блокується доступ до деякого ресурсу обчислювальної системи.

Несанкціонований доступ до інформації і його мета

Спосіб несанкціонованого доступу (НСД) – це сукупність прийомів і порядок дій з метою одержання інформації, що охороняється, незаконним протиправним шляхом і забезпечення можливості впливати на цю інформацію (наприклад: підмінити, знищити).

При здійсненні несанкціонованого доступу, зловмисник переслідує три мети:

• одержати необхідну інформацію для конкурентної боротьби;

• мати можливість вносити зміни в інформаційні потоки конкурента у відповідності зі своїми інтересами;

• завдати шкоди конкурентові шляхом знищення матеріалу інформаційних цінностей.

Повний обсяг даних про діяльність конкурента не може бути отриманий тільки яким – небудь одним з можливих способів доступу до інформації. Від мети залежить як вибір способів дій, так і кількісний і якісний склад сил і засобів одержання інформації.

Порушники безпеки інформації

Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як *«комп'ютерне піратство»*.

Для запобігання можливих загроз, фірми повинні не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але спробувати виявити категорії порушників і методи, які вони використовують.

Залежно від мотивів, мети та методів, дії порушників безпеки інформації можна поділити на чотири категорії:

• шукачі пригод;

• ідейні «хакери»;

• «хакери» - професіонали;

• ненадійні (неблагополучні) співробітники.

Рис. 1.2 Способи НСД до конфіденційної інформації

Шукач пригод, як правило, студент або старшокласник, і в нього є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись із ускладненнями. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями – колегами.

Ідейний «хакер» - це той же шукач пригод, але більш майстерний. Він уже вибирає собі конкретні цілі (хости і ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення Web-сервера або, блокування роботи ресурсу, що атакується. У порівнянні із шукачем пригод, ідейний «хакер» розповідає про успішні атаки набагато більшій аудиторії, звичайно розміщаючи інформацію на хакерському Web - вузлі.

«Хакер»-професіонал має чіткий план дій і спрямовує його на визначені ресурси. Його атаки добре продумані і, звичайно, здійснюються у кілька етапів. Спочатку він збирає попередню інформацію (тип ОС, надані сервіси і міри захисту). Потім він складає план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Далі, провівши атаку, він одержує закриту інформацію і, нарешті, знищує всі сліди своїх дій. Такий професіонал звичайно добре фінансується і може працювати один або у складі команди професіоналів.

Ненадійний (неблагополучний) співробітник своїми діями може спричинити стільки ж проблем (буває і більше), скільки промисловий шпигун, до того ж, його присутність звичайно складніше знайти. Крім того, йому доводиться долати не зовнішній захист мережі, а тільки, як правило, менш жорсткіший, внутрішній. Він не такий витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки, і тим самим може видати свою присутність. Однак, у цьому випадку, небезпека його несанкціонованого доступу до корпоративних даних набагато вища, ніж будь – якого іншого зловмисника.

Перераховані категорії порушників безпеки інформації можна згрупувати за їхньою кваліфікацією: початківець (шукач пригод), фахівець (ідейний «хакер», ненадійний співробітник), професіонал («хакер»-професіонал). А якщо з цими групами зіставити мотиви порушення безпеки і технічну забезпеченість кожної групи, то можна одержати узагальнену модель порушника безпеки інформації, як це показано на рис. 1.3.

Порушник безпеки інформація, як правило, будучи фахівцем визначеної кваліфікації, намагається довідатися все про комп'ютерні системи і мережі, зокрема, про засоби їх захисту. Тому модель порушника визначає:

- категорії осіб, у числі яких може виявитися порушник;
- можливі цілі порушника і їх градації за ступенем важливості та небезпеки;
- припущення про його кваліфікації;
- оцінка його технічної озброєності;
- обмеження і припущення про характер його дій.

Діапазон спонукальних мотивів одержання доступу до системи досить широкий: від бажання випробувати емоційний підйом під час гри із комп'ютером до відчуття влади над ненависним менеджером. Займаються цим не тільки новачки, що бажають побавитися, але і професійні програмісти. Паролі вони добувають або у результаті підбору, або здогадування, або шляхом обміну з іншими « хакерами».

Частина з них, однак, починає не тільки переглядати файли, але і виявляти інтерес саме до їх змісту, а це вже спричиняє серйозну загрозу, оскільки у даному випадку важко відрізнити звичайну цікавість від злочинних дій.

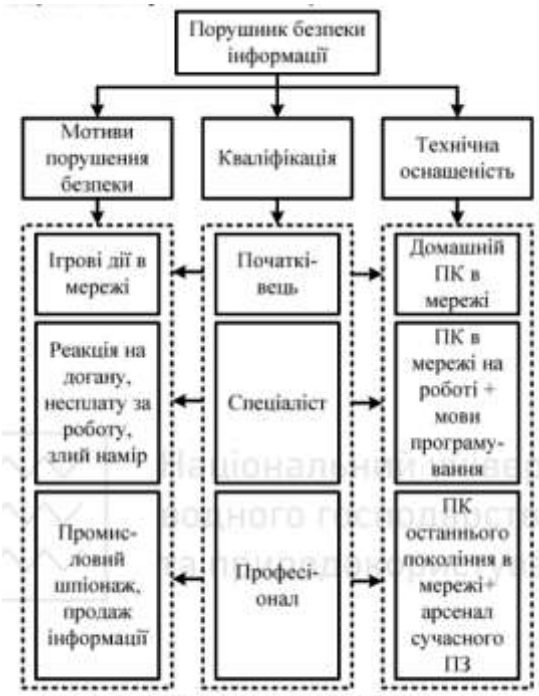

Рис. 1.3 Модель порушника безпеки інформації.

Донедавна викликали занепокоєння випадки, коли незадоволені керівником службовці, зловживаючи своїм положенням, псували системи, допускаючи до них сторонніх або залишаючи системи без догляду в робочому стані. Спонукальними мотивами таких дій є:

• реакція на догану або зауваження з боку керівника;

• невдоволення тим, що фірма не оплатила понаднормові години роботи (хоча найчастіше понаднормова робота виникає через неефективне використання робочого часу);

• злий намір у якості, наприклад, реваншу з метою послабити фірму як конкурента якої – небудь новоствореної фірми.

Професійні «хакери» - це комп'ютерні фанати, що прекрасно знають обчислювальну техніку і системи зв'язку. Вони затратили масу часу на обмірковування способів проникнення в системи і ще більше, експериментуючи із самими системами. Для входження в систему професіонали найчастіше використовують деяку систематичність та експерименти, а не розраховують на удачу або інтуїцію. Їх мета – виявити і перебороти захист, вивчити можливості обчислювальної установки і потім вийти з неї, довівши можливість досягнення своєї мети.

До категорії хакерів – професіоналів звичайно відносять наступних осіб:

• таких, що входять у злочинні угруповання, які переслідують політичні цілі;

• прагнучих одержати інформацію з метою промислового шпигунства;

• «хакер» або угруповання «хакерів», що прагнуть до наживи.

Сьогодні, зі стрімким розвитком Internet, «хакери» стають справжньою загрозою для державних і корпоративних комп'ютерних мереж. Так, за оцінками експертів США, напади «хакерів» на комп'ютери і мережі федеральних державних систем відбуваються в цій країні не рідше 50 – ти раз на день. Багато великих компаній і організації піддаються атакам кілька разів у тиждень, а деякі навіть щодня. Виходять такі атаки не завжди ззовні, 70% спроб зловмисного проникнення в комп'ютерні системи мають джерело всередині самої організації

ТЕМА Основи безпеки даних в комп’ютерних системах.

Як вважають західні фахівці, витік 20% комерційної інформації в 60 випадках з 100 призводить до банкрутства фірми. Жодна, навіть процвітаюча фірма не проіснує більше трьох діб, якщо її інформація, що складає комерційну таємницю, стане відомою. Таким чином, економічна та інформаційна безпека виявляються тісно взаємозалежними.

Збитки від діяльності конкурентів, що використовують методи шпигунства, складають у світі до 30% усього збитку, а це мільярди доларів. Точну цифру збитків указати не можна внаслідок того, що ні злочинці, ні потерпілі не прагнуть піддавати гласності зроблені дії. Перші, мабуть, через страх відповідальності за вчинене, а другі – через страх втратити імідж. Цим пояснюється високий рівень латентності правопорушень і відсутність інформації про них в засобах масової інформації. Тому до публіки доходить менш 1% від усіх випадків порушень, що мають карний характер і які приховати неможливо.

Таким чином, задачі безпеки будь-яких видів доводиться вирішувати щораз при розгляді всіляких аспектів людської діяльності. Але, як бачимо, всі види безпеки тісно пов’язані з інформаційною безпекою (ІБ) і, більш того, їх неможливо забезпечити без забезпечення ІБ. Отже, предметом нашого подальшого розгляду буде саме захист інформації в інформаційних автоматизованих системах.

Особливістю терміну “інформація” є те, що, з одного боку, він є інтуїтивно зрозумілим практично для всіх, а з іншого боку – загальновизнаного його трактування в науковій літературі не існує. Одночасно слід особливо зазначити, що як наукова категорія “інформація” складає предмет вивчення для всіляких областей знань: філософії, інформатики, кібернетики і т.д.

Інформація – це відомості про осіб, факти, предмети, події, явища і процеси, незалежно від форми їх уявлення.

Захист інформації – комплекс заходів, проведених із метою запобігання (зниження до безпечного рівня) можливостей витікання, розкрадання, втрати, поширення, знищення, перекручування, підробки або блокування інформації.

Для правильної побудови системи захисту необхідно визначити:

1. Види дій над інформацією.

2. Що з себе являє автоматизована система.

3. Які існують загрози безпеки автоматизованих систем.

4. Заходи протидії загрозам безпеки.

5. Принципи побудови систем захисту.

Види дій над інформацією:

1. Блокування інформації (користувач не може дістати доступ до інформації; за відсутності доступу сама інформація не втрачається).

Причини: відсутність устаткування, фахівця, програмного забезпечення.

2. Порушення цілісності (втрата, вихід з ладу носія; спотворення, тобто порушення смислової значущості; порушення логічної зв'язаності; втрата достовірності (наявна інформація не відповідає реальному стану)).

3. Порушення конфіденційності (з інформацією ознайомлюються суб'єкти, на яких це не покладено).

Рівень допуску до інформації визначає її власник. Порушення конфіденційності може відбутися із-за неправильної роботи системи обмеження доступу або наявності побічного каналу доступу.

4. Несанкціоноване тиражування (під захистом розуміється захист авторських прав і прав власності на інформацію).

Автоматизована система (АС) – це організаційно-технічна система, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію.

Захист інформації в АС (information protection, information security, computer system security) – діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС у цілому і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Причини пошкодження інформації: 79% - низька кваліфікація користувачів; 20% - заплановані розкрадання; 1% - віруси.

Типові структури АС:

1. Автономні робочі станції (один або декілька ПК, не зв'язаних між собою. На будь-якому з них користувачі працюють роздільно в часі. Обмін інформацією відбувається тільки через змінні носії (дискети, диски)).

Об'єкти захисту в автономних робочих станціях:

- власне робоча станція;

- змінні носії інформації;

- користувачі і робочий персонал;

- пристрої візуального представлення інформації (монітор, принтер тощо);

- прилади-джерела побічних електромагнітних випромінювань і наведень.

2. Локальні системи колективного користування (створюються для колективної обробки інформації і (або) сумісного використання ресурсів; устаткування розміщене в межах одного приміщення, будівлі або групи близько розташованих будівель).

Структури локальних систем колективного користування:

1. Без виділеного сервера (однорангові мережі) (не вимагають централізованого управління; будь-який користувач сам робить свої ресурси доступними іншим; використовується однотипна операційна система (ОС)).

2. З виділеним сервером/серверами (побудовані на робочих станціях і серверах; вимагають централізованого адміністративного управління).

3. Багато термінальні системи на базі малих і великих комп'ютерів (основні ресурси зосереджені на сервері. Робочі станції – термінали. Загальне керівництво здійснює адміністратор. На центральному комп'ютері і робочих станціях використовуються різні ОС).

4. Багато сегментні локальні мережі (складаються з декількох сегментів, будь-який з яких є мережею з виділеним сервером. Об'єднання здійснюється через міст, в якості якого може використовуватися або виділений сервер, або спеціальний пристрій. Будь-яким сегментом управляє свій адміністратор. У будь-якому сегменті може використовуватися своя ОС).

5. Змішані мережі (включають всі раніше розглянуті системи).

Об'єкти захисту:

- всі робочі станції;

- виділені сервери і центральний комп'ютер;

- локальні канали зв'язку;

- реквізити доступу.

6. Глобальні системи колективного користування (розміщені на значній відстані один від одного; об'єднані через глобальні канали зв'язку, які не належать власнику).

Використовуються для сумісної обробки інформації і сумісного використання ресурсів.

Відмінності від локальних систем:

- можуть знаходитися на значній відстані одна від одної;

- канали зв'язку не належать власнику системи;

- канали зв'язку є комутованими і взаємозв'язаними;

- для використання каналів зв'язку необхідний пристрій сполучення;

- подібні системи відкриті і підключитися до ним можуть всі охочі.

Об’єкти захисту включають в себе все те ж, що й в локальних системах колективного користування, а також:

1. глобальні канали зв’язку;

2. інформація, що передається по глобальних каналах зв’язку;

3. інформація про реквізити доступу в глобальні системи колективного користування.

Загрози безпеки даних та їх особливості

Загроза – потенційно можлива подія, дія, процес або явище, яке може привести до нанесення збитку інтересам певної фізичної чи юридичної особи.

Реалізацією загрози є порушення роботи системи. Загрози поділяються на природні та штучні.

Природні загрози – загрози, викликані дією на АС об’єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози – такі, що викликані діяльністю людини.

Природні загрози – це стихійні лиха, магнітні бурі, радіоактивне випромінювання, опади тощо, а також загрози опосередковано технічного характеру, пов’язані з надійністю технічних засобів обробки інформації і підсистем забезпечення АС.

Штучні поділяються на:

1. ненавмисні – загрози, пов’язані з випадковими діями людей, через незнання, халатність, цікавість, але без злого наміру.

Наприклад: ненавмисне псування носіїв інформації; запуск програм, не передбачених службовою необхідністю; необережні дії, що призводять до розголошування конфіденційної інформації; розголошування реквізитів доступу в АС; псування каналів зв’язку.

2. навмисні – дії людини, що здійснюються умисне для дезорганізації роботи системи, виведення її з ладу, для незаконного проникнення в систему і несанкціонованого доступу до інформації.

Наприклад: фізичне знищення системи; розкрадання носіїв інформації; читання залишкової інформації з ОЗП; несанкціоноване копіювання; вербування персоналу тощо.

ТЕМА Основні шляхи забезпечення безпеки інформації.

Вразливість інформації в автоматизованих комплексах обумовлена великою концентрацією обчислювальних ресурсів, їх територіальною розподіленістю, довгостроковим збереженням великого об’єму даних на магнітних та оптичних носіях, одночасним доступом до ресурсів багатьох користувачів. У цих умовах необхідність вживання заходів захисту, напевно, не викликає сумнівів. Однак існують певні труднощі:

• немає єдиної теорії захисту систем;

• виробники засобів захисту, в основному, пропонують окремі компоненти для рішення приватних задач, залишаючи питання формування системи захисту і сумісності цих засобів на розсуд споживачів;

• для забезпечення надійного захисту необхідно розв’язати цілий комплекс технічних і організаційних проблем і розробити відповідну документацію.

Для подолання перерахованих вище труднощів, необхідна координація дій всіх учасників інформаційного процесу як на окремому підприємстві, так і на державному рівні.

Концепція захисту інформації – офіційно прийнята система поглядів на проблему інформаційної безпеки і шляхи її рішення з урахуванням сучасних тенденцій. Вона є методологічною основою політики розробки практичних заходів для її реалізації. На базі сформульованих у концепції цілей, задач і можливих шляхів їх рішення формуються конкретні плани забезпечення інформаційної безпеки.

Стратегія та архітектура захисту інформації

В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту.

Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки. Можна виділити два основних напрямки:

• аналіз засобів захисту;

• визначення факту вторгнення.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації (рис.2.1).

Рис. 2.1 Ієрархічний підхід до забезпечення безпеки інформації

Розробку концепції захисту рекомендується проводити в три етапи (рис. 2.2).

На першому етапі повинна бути чітко визначена цільова установка захисту, тобто які реальні цінності, виробничі процеси, програми, масиви даних необхідно захищати. На цьому етапі доцільно диференціювати за значимістю окремі об'єкти, що вимагають захисту.

На другому етапі повинен бути проведений аналіз злочинних дій, що потенційно можуть бути зроблені стосовно об'єкта, що захищається. Важливо визначити ступінь реальної небезпеки таких найбільш широко розповсюджених злочинів, як економічне шпигунство, саботаж, крадіжки зі

зломом. Потім потрібно проаналізувати найбільш ймовірні дії зловмисників стосовно основних об'єктів, що потребують захисту.

Рис. 2.2 Етапи розробки концепції захисту інформації

Головною метою третього етапу є аналіз обставин, у тому числі місцевих специфічних умов, виробничих процесів, уже встановлених технічних засобів захисту.

Концепція захисту повинна містити перелік організаційних, технічних і інших заходів, що забезпечують максимальну безпеку при заданому залишковому ризику і мінімальні витрати на їх реалізацію.

Політика захисту – це загальний документ, де перераховуються правила доступу, визначаються шляхи реалізації політики та описується базова архітектура середовища захисту.

Власне документ складається із декількох сторінок тексту. Він формує основу фізичної архітектури мережі, а інформація, що знаходиться в ньому, визначає вибір продуктів захисту. При цьому, документ може і не включати список необхідних закупок, але вибір конкретних компонентів після його складання повинен бути очевидним.

Політика захисту повинна обов'язково включати наступне:

• контроль доступу (заборона на доступ користувача до матеріалів, якими йому не дозволено користуватися);

• ідентифікацію та аутентифікацію (використання паролів або інших механізмів для перевірки статусу користувача);

• облік (запис усіх дій користувача в мережі);

• контрольний журнал (журнал дозволяє визначити, коли і де відбулося порушення захисту);

• акуратність (захист від будь – яких випадкових порушень);

• надійність (запобігання монополізації ресурсів системи одним користувачем);

• обмін даними (захист усіх комунікацій).

Один з найпростіших способів реалізувати захист – доручити зайнятися цим спеціалізованій компанії.

Політика безпеки інформації.

Розробляючи політику безпеки інформації, спочатку визначають об'єкти, які треба захистити, і їх функції. Потім оцінюють ступінь інтересу потенційного супротивника до цих об'єктів, ймовірні види нападу і спричинений ними збиток. Нарешті, визначають вразливі для впливу області, в яких наявні засоби протидії не забезпечують достатнього захисту. При цьому, розробка політики безпеки

інформації повинна проводитися з урахуванням задач, рішення яких забезпечить реальний захист даного об'єкта (рис. 2.3).

Автоматизований комплекс можна вважати захищеним, якщо всі операції виконуються у відповідності з чітко визначеними правилами (рис. 2.4), що забезпечують безпосередній захист об'єктів, ресурсів і операцій. Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту. Ці правила, в свою чергу, визначають необхідні функції і заходи захисту. Чим суворіші вимоги до захисту і більше відповідних правил, тим ефективніші його механізми і тим більш захищеним виявляється автоматизований комплекс.

Отже, захист інформації в комп'ютерній мережі ефективніший в тому випадку, коли проектування і реалізація системи захисту відбувається в **три етапи:**

• аналіз ризику;

• реалізація політики безпеки;

• підтримка політики безпеки.

На першому етапі аналізуються вразливі елементи комп'ютерної мережі, визначаються й оцінюються загрози і підбираються оптимальні засоби захисту. Аналіз ризику закінчується прийняттям політики безпеки. **Політикою безпеки (Security Policy)** називається комплекс взаємозалежних засобів, спрямованих на забезпечення високого рівня безпеки. **У теорії захисту інформації вважається, що ці засоби повинні бути спрямовані на досягнення наступних цілей:**

• конфіденційність (засекречена інформація повинна бути доступна тільки тому, кому вона призначена);

• цілісність (інформація, на основі якої приймаються рішення, повинна бути достовірною і повною, а також захищена від можливих ненавмисного і злочинного перекручувань);

• готовність (інформація і відповідні автоматизовані служби повинні бути доступні та, у разі потреби, готові до обслуговування).

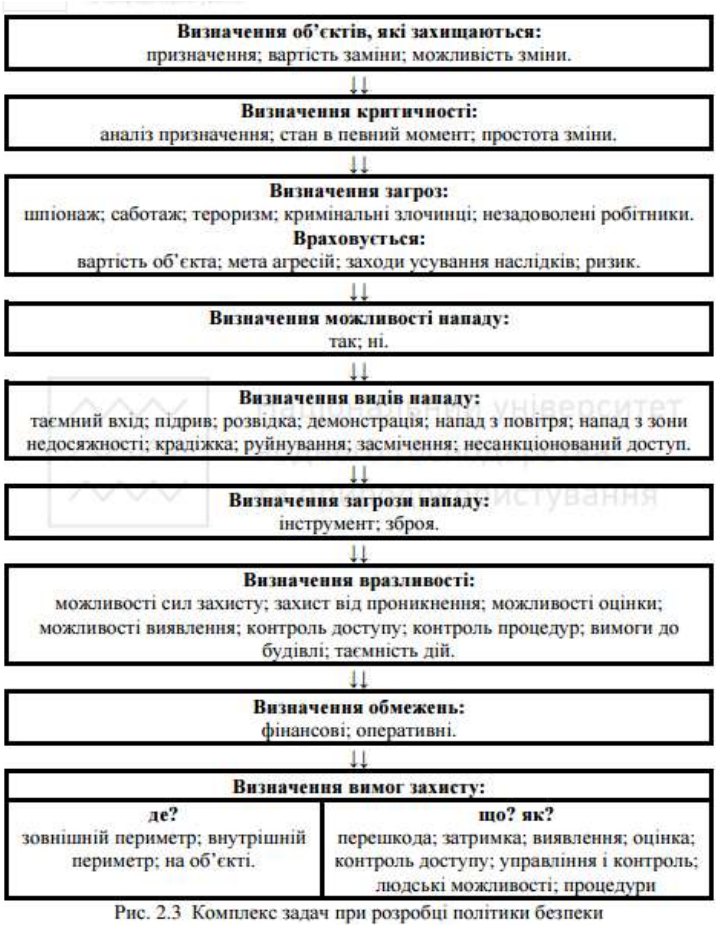

Рис. 2.3 Комплекс задач при розробці політики безпеки

Рис. 2.4 Основні правила забезпечення політики безпеки інформації

Вразливість означає невиконання хоча б однієї з цих властивостей. Для комп'ютерних мереж можна виділити наступні ймовірні загрози, які необхідно враховувати при визначенні політики безпеки:

• несанкціонований доступ сторонніх осіб, що не належать до числа службовців і ознайомлення зі збереженою конфіденційною інформацією;

• ознайомлення своїх службовців з інформацією, до якої вони не повинні мати доступу;

• несанкціоноване копіювання програм і даних;

• перехоплення та ознайомлення з конфіденційною інформацією, переданої по каналах зв'язку;

• крадіжка магнітних носіїв, що містять конфіденційну інформацію;

• крадіжка роздрукованих документів;

• випадкове або навмисне знищення інформації;

• несанкціонована модифікація службовцями документів і баз даних;

• фальсифікація повідомлень, переданих по каналах зв'язку;

• відмова від авторства повідомлення, переданого по каналах зв'язку;

• відмовлення від факту одержання інформації;

• нав'язування раніше переданого повідомлення;

• помилки в роботі обслуговуючого персоналу;

• руйнування файлової структури через некоректну роботу програм або апаратних засобів;

• руйнування інформації, викликане вірусними впливами;

• руйнування архівної інформації, що зберігається на магнітних носіях;

• крадіжка устаткування ;

• помилки в програмному забезпеченні;

• відключення електроживлення;

•збої устаткування.

Оцінка імовірності появи даних погроз і очікуваних розмірів втрат – важка задача. Ще складніше визначити вимоги до системи захисту. **Політика безпеки повинна визначатися наступними заходами:**

• ідентифікація, перевірка дійсності і контроль доступу користувачів на об'єкт, у приміщення, до ресурсів автоматизованого комплексу;

• поділ повноважень користувачів, що мають доступ до обчислювальних ресурсів;

• реєстрація та облік роботи користувачів;

• реєстрація спроб порушення повноважень;

• шифрування конфіденційної інформації на основі криптографічних алгоритмів високої стійкості;

• застосування цифрового підпису для передачі інформації по каналах зв'язку;

• забезпечення антивірусного захисту (у тому числі і для боротьби з невідомими вірусами) і відновлення інформації, зруйнованої вірусними впливами;

• контроль цілісності програмних засобів і оброблюваної інформації;

• відновлення зруйнованої архівної інформації, навіть при значних втратах;

• наявність адміністратора (служби) захисту інформації в системі;

• вироблення і дотримання необхідних організаційних заходів;

• застосування технічних засобів, що забезпечують безперебійну роботу устаткування.

Другий етап – реалізація політики безпеки – починається з проведення розрахунку фінансових витрат і вибору відповідних засобів для виконання цих задач. При цьому, необхідно врахувати такі фактори як: безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії. Крім того, варто враховувати принципи, в яких відображені основні положення по безпеці інформації:

• економічна ефективність (вартість засобів захисту повинна бути меншою, ніж розміри можливого збитку);

• мінімум привілей (кожен користувач повинен мати мінімальний набір привілей, необхідних для роботи);

• простота (захист буде тим ефективніший, чим легше користувачеві з ним працювати);

• відключення захисту (при нормальному функціонуванні захист не повинен відключатися, за винятком особливих випадків, коли співробітник зі спеціальними повноваженнями може мати можливість відключити систему захисту);

• відкритість проектування і функціонування механізмів захисту (таємність проектування і функціонування засобів безпеки – кращий підхід до захисту інформації тому, що фахівці, які мають відношення до системи захисту, повинні цілком уявляти собі принципи її функціонування та, у випадку виникнення скрутних ситуацій, адекватно на них реагувати);

• незалежність системи захисту від суб'єктів захисту (особи, що займалися розробкою системи захисту, не повинні бути в числі тих, кого ця система буде контролювати);

• загальний контроль (будь – які виключення з безлічі контрольованих суб'єктів і об'єктів захисту знижують захищеність автоматизованого комплексу);

• звітність і підконтрольність (система захисту повинна надавати досить доказів, що показують коректність її роботи);

• відповідальність (особиста відповідальність осіб, що займаються забезпеченням безпеки інформації);

• ізоляція і поділ (об'єкти захисту доцільно розділяти на групи таким чином, щоб порушення захисту в одній з груп не впливало на безпеку інших груп);

• відмова за замовчуванням (якщо відбувся збій засобів захисту і розроблювачі не передбачили такої ситуації, то доступ до обчислювальних ресурсів повинен бути заборонений);

• повнота і погодженість (система захисту повинна бути цілком специфікована, протестована і погоджена);

• параметризація (захист стає більш ефективним і гнучкішим, якщо він допускає зміну своїх параметрів з боку адміністратора);

• принцип ворожого оточення (система захисту повинна проектуватися в розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, що вони будуть робити серйозні помилки і шукати шляхи обходу механізмів захисту);

• залучення людини (найбільш важливі і критичні рішення повинні прийматися людиною, тому що комп'ютерна система не може передбачити всі можливі ситуації);

• відсутність зайвої інформації про існування механізмів захисту (існування механізмів захисту повинно бути по можливості приховане від користувачів, робота яких контролюється).

Підтримка політики безпеки – третій, найбільш важливий, етап. Заходи, проведені на даному етапі, вимагають постійного спостереження за вторгненнями у мережу зловмисників,

виявлення «дір» у системі захисту об'єкта інформації, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку політики безпеки мережі лежить на системному адміністраторі, що повинен оперативно реагувати на усі випадки злому конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні і програмні засоби захисту з урахуванням максимальної економії фінансових засобів.

Види забезпечення безпеки інформації

В даний час комп'ютерні злочини надзвичайно різноманітні. Це несанкціонований доступ до інформації, що зберігається в комп'ютері, розробка і поширення комп'ютерних вірусів, розкрадання комп'ютерної інформації, недбалість у розробці, виготовленні та експлуатації програмно – обчислювальних комплексів, підробка комп'ютерної інформації.

Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, *можна поділити на:*

• правові;

• організаційно - адміністративні;

• інженерно - технічні.

До правових заходів (рис. 2.5) варто віднести розробку норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалювання карного і цивільного законодавства, а також судочинства. До них відносяться також питання суспільного контролю за розроблювачами комп'ютерних систем і прийняття відповідних міжнародних договорів про обмеження, якщо вони впливають або можуть уплинути на військові, економічні і соціальні аспекти країн. Тільки в останні роки з'явилися роботи з проблем правової боротьби з комп'ютерними злочинами.

Рис. 2.5 Правові норми забезпечення безпеки інформації

До організаційно – адміністративних заходів (рис. 2.6) відносяться: охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх

користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру.

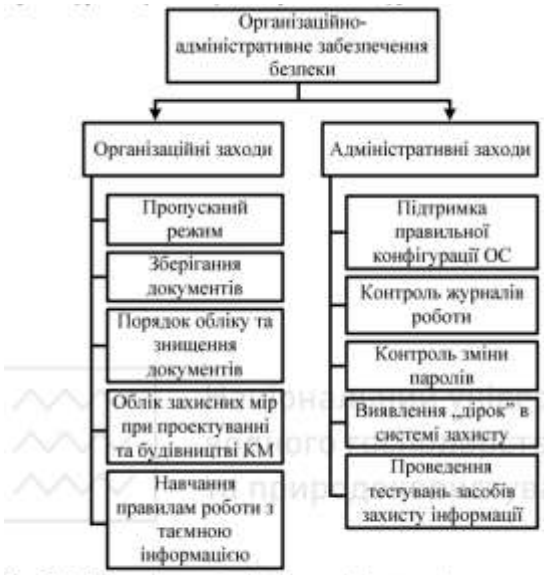

Рис. 2.6 Основні організаційні та адміністративні заходи по захисту інформації в мережі.

До інженерно – технічних заходів (рис. 2.7) можна віднести захист від несанкціонованого доступу до комп'ютерної системи, резервування важливих комп'ютерних систем, забезпечення захисту від розкрадань і диверсій, резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо.

Фізичні засоби містять у собі різні інженерні засоби, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту, що захищають персонал (особисті засоби безпеки), матеріальні засоби і фінанси, інформацію від протиправних дій.

До апаратних засобів відносяться прилади, пристрої, пристосування та інші технічні рішення, які використовуються в інтересах забезпечення безпеки. У практиці діяльності будь – якої організації знаходить широке застосування різна апаратура: від телефонного апарату до розроблених автоматизованих інформаційних систем, що забезпечують її виробничу діяльність. Основна задача апаратних засобів – стійка безпека комерційної діяльності.

Рис. 2.7 Основні інженерні та технічні заходи по захисту інформації в мережі

Програмні засоби – це спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки даних.

Криптографічні засоби – це спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування.