Львівський державний університет безпеки життєдіяльності

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Лекція
на тему: " Вступ до предмету. Основні поняття"

(для курсантів та студентів 5-го курсу спеціальності «Комп'ютерні науки»)

ПЛАН ЛЕКЦІЇ

1. Вступ.
2. Термінологія.
3. Завдання захисту та загрози безпеці інформації.
4. Класифікація атак.
5. Модель порушника

ЛІТЕРАТУРА

1. **Богуш В.М., Кудін А.М.** Інформаційна безпека від А до Я. - К.: МОУ, 1999. – 456 с.

2. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.

3. **Зегжда Д.П., Ивагико А.М.** Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2000. – 452 с.

4. **Прохоров И.В., Толстой А.И.** Телекоммуникационные сети: Учебное пособие. – М.: МИФИ, 1996. – 64 с.

1. Вступ.

Будь-яка інформація, незалежно від того, чи є вона власністю держави, всього суспільства або окремих організацій чи фізичних осіб, становить певну цінність. Відтак інформаційні ресурси потребують захисту від різних впливів, які можуть призвести до зниження їхньої цінності.

Здавна люди розв'язували питання захисту інформації, переважно – державних і військових таємниць. Завдання захисту були досить типовими і не змінювалися протягом тисячоліть - забезпечити передавання інформації від достовірного джерела вповноваженій особі так, щоб вона не потрапила до інших осіб.

Для цього використовували різні методи захисту. Деякі з них із незначними змінами застосовують і зараз, коли, наприклад, підтверджують справжність документа особистою печаткою. Були й такі методи, що сьогодні виглядають досить дивними і жорстокими, - відсікання голови посланцю, який передав усне повідомлення, щоб той не міг в подальшому переповісти його будь-кому. Вже тоді почали винаходити способи таємного записування інформації, щоб лише уповноважені особи могли зрозуміти зміст надісланих їм повідомлень.

У XXI столітті правила роботи з таємною інформацією, способи її зберігання, передавання, а також методи ведення розвідки з метою здобуття такої інформації не уповноваженими (ворожими) особами зазнали суттєвих змін через бурхливий розвиток технічних засобів, що використовували як для захисту інформації, так і для подолання цього захисту. Наприкінці XX століття було здійснено чергову технічну революцію, яка стосувалася саме технологій підготовки, зберігання, пошуку, оброблення та розповсюдження інформації. Йдеться про масове застосування комп'ютерної техніки, що стала загальнодоступною, а також про об'єднання комп'ютерів у мережі, які досягли глобального масштабу. В результаті виникли і набули поширення розподілені інформаційні системи, які дістали назву інформаційно- комунікаційних систем.

Можна було б припустити, що питання захисту цифрової інформації можна вирішувати тими самими методами, що застосовували для захисту традиційних (паперових) носіїв інформації. Певною мірою це дійсно так.

Але є й інший бік проблеми. Комп'ютерна технологія оброблення інформації несе в собі певні загрози, які можуть призвести до небажаних втрат або тимчасової недоступності важливих даних. Зрештою, будь-яка нова технологія приховує небезпеку, яка не завжди очевидна. Можна навести безліч прикладів з історії розвитку техніки, коли під час бурхливого впровадження певної технології питання безпеки спочатку не дуже цікавили людство, а потім ставали пріоритетними (це стосується автомобільного та авіаційного транспорту), а в деяких випадках навіть критичними для його існування (наприклад, атомна енергетика, хімічна промисловість).

У контексті інформаційно-комунікаційних систем слід згадати системи зберігання даних, надійність яких власники інформації інколи переоцінюють. Але є й менш очевидні проблеми. Зокрема, це можливість (на жаль, реалізована на практиці) існування шкідливого і навіть руйнівного програмного забезпечення. Передумовою його існування є унеможливлення або суттєве ускладнення перевірки всіх функцій програмного забезпечення. Це означає, що програми можуть містити так звані недокументовані функції - приховані функції, реалізовані програмістами та навмисно або через їхню недбалість долучені до програмного продукту і не описані в

документації. Такі функції можуть бути активізовані випадково (за збігу обставин, внаслідок помилок чи збоїв) або навмисно (за певних умов). Одним із найпоширеніших і найнебезпечніших різновидів шкідливого програмного забезпечення є комп'ютерні віруси, здатні розмножуватись і розповсюджуватись.

З усього цього можна зробити один важливий висновок - без застосування спеціальних заходів захисту існує дуже висока ймовірність пошкодження інформації в інформаційно-комунікаційній системі, що може завдати збитків її власнику.

Отже, задачі захисту інформації в інформаційно-комунікаційній системі є суперпозицією задач двох головних напрямів:

- захист важливої інформації, зокрема державної, військової або комерційної таємниці, від цілеспрямованих дій порушників;
- захист інформації від впливів, спричинених некоректним функціонуванням комп'ютерної системи через відмови обладнання, збої програмного забезпечення, помилки в реалізації апаратних або програмних засобів, або наявність програмних засобів з прихованими руйнуючими властивостями.

2. Термінологія

У сфері захисту інформації, як і в будь-якій іншій сфері діяльності, існує специфічна термінологія (професійна і жаргонна), що відображає концептуальні підходи до розв'язання конкретних проблем. Відтак ми розпочнемо саме з неї. Ми розглянемо основні терміни та наведено їх тлумачення.

Розгляд термінології доцільно почати з визначення систем, в яких здійснюється захист інформації.

Інформаційно-телекомунікаційна система

Інформаційно-телекомунікаційною системою (ІТС) називають організаційно-технічну систему, яка виконує функції інформаційної системи, тобто такої організаційно-технічної системи, що реалізує певну технологію (або сукупність технологій) оброблення інформації, та (або) телекомунікаційної системи — технічної системи, що реалізує певну технологію (або сукупність технологій) передавання даних шляхом їх кодування у формі фізичних сигналів.

Комп'ютерна система

Термін «комп'ютерна система» (КС) часто використовують як узагальнюючий, його виносять у заголовки статей, книжок і навіть нормативних документів. Але у вітчизняних нормативних документах тлумачення цього терміну досить специфічне. Згідно з Нормативним документом в галузі технічного захисту інформації НД ТЗІ 1.1-003-99 «Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу», ***комп'ютерна система*** — це сукупність програмно-апаратних засобів, яку подають на оцінювання. Під оцінюванням тут розуміють експертне оцінювання захищеності інформації в системі, яке є складовою експертизи або сертифікації на відповідність чинним нормативним документам і стандартам. Таке оцінювання ще називають кваліфікаційним аналізом. Термін «комп'ютерна система» у НД ТЗІ вживають до об'єктів оцінювання різних класів як узагальнення термінів «обчислювальна система» та «автоматизована система».

Обчислювальна система

Під ***обчислювальною системою*** розуміють сукупність програмних і апаратних засобів, призначених для оброблення інформації. Обчислювальна система поєднує в собі технічні засоби оброблення і передавання даних (засоби обчислювальної техніки

і зв'язку), а також методи і алгоритми оброблення даних, реалізовані у вигляді відповідного програмного забезпечення (ПЗ).

Позаяк в українській мові стандартна абревіатура для обчислювальної системи (ОС) збігається з більш поширеною абревіатурою для операційної системи - найважливішого програмного компонента будь-якої обчислювальної системи (зокрема, в контексті захисту інформації), ми уникатимемо використання цієї абревіатури для обчислювальних систем, вживаючи її до операційних систем.

Автоматизована система

Термін «автоматизована система» вживають до систем автоматизованого оброблення інформації, побудованих на основі обчислювальної техніки. Його використовують не лише в контексті захисту оброблюваної інформації, але й в численних стандартах, наприклад ГОСТ серії 34 (Інформаційна технологія. Комплекс стандартів на автоматизовані системи).

Є різні тлумачення терміну «автоматизована система». Ми дотримуватимемося визначення з НД ТЗІ 1.1-003-99 : ***автоматизована система*** **(АС)** — це організаційно-технічна система (рис. 1.1), що реалізує інформаційну технологію і поєднує у собі:

- обчислювальну систему;
- фізичне середовище;
- персонал;
- інформацію, яка обробляється.

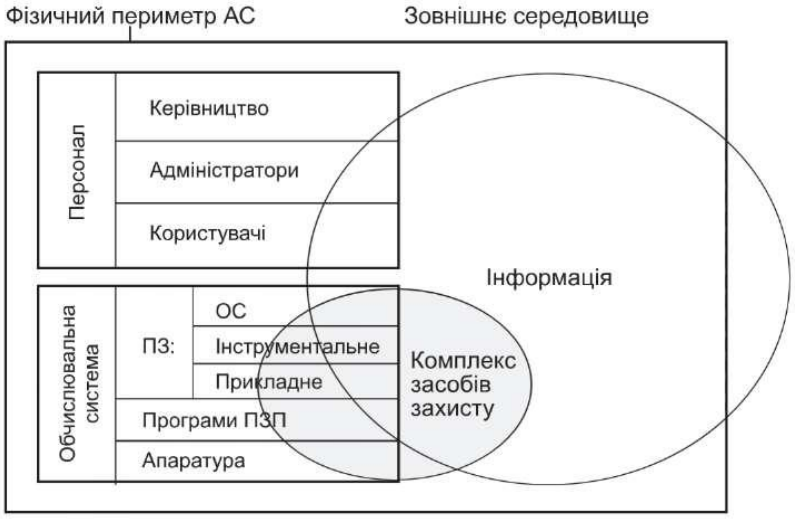


Рис. 1.1. Структура автоматизованої системи

Отже, обчислювальна система, персонал, інформація з технологією її оброблення та фізичне середовище є складовими АС. Також ці компоненти часто називають середовищем функціонування системи.

Також слід усвідомлювати, що не реалізація інформаційно-комунікаційної системи дає можливість користувачам різних категорій звертатися до певних інформаційних ресурсів, а зовнішні чинники, до яких насамперед належать Закони України (або іншої держави, відповідно до того правового поля, в якому функціонуватиме система). З усього цього випливає найважливіше для визначення мети захисту інформації поняття — політика безпеки.

Політика безпеки [інформації] — це сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації в

ІКС. Таким чином, саме політика безпеки інформації обумовлює вживання тих чи інших заходів захисту, які дають змогу підтримувати безпеку інформації.

Безпека інформації — це стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. Багаторічний досвід захисту інформації в ІКС дозволив визначити головні властивості інформації, збереження яких дає змогу гарантувати збереження цінності інформаційних ресурсів. Це конфіденційність, цілісність і доступність інформації.

Конфіденційність — властивість інформації, завдяки якій лише вповноважені користувачі мають змогу її отримувати (тобто ознайомлюватися з інформацію).

Цілісність — властивість інформації, яка дає можливість лише вповноваженим користувачам її модифікувати.

Доступність — властивість інформації, завдяки якій уповноважені користувачі можуть використовувати її згідно з правилами, встановленими політикою безпеки, не очікуючи довше заданого (невеликого) проміжку часу. Тобто інформаційний ресурс має необхідний користувачу вигляд, знаходиться в тому місці, де це потрібно користувачу, і тоді, коли це йому потрібно.

Термін *доступність* вживають не лише, коли йдеться про інформаційні ресурси, але й до ІКС у цілому, до її компонентів або окремих ресурсів. Наприклад, коректно говорити про доступність сервера, сегмента мережі, служби електронної пошти тощо.

3. Завдання захисту та загрози безпеці інформації.

Далі ми зосередимо увагу на термінах, безпосередньо пов'язаних із питаннями захисту інформації в ІКС, при цьому будемо дотримуватися термінології згідно з НД ТЗІ 1.1-003-99 та ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення» . Перше питання, яке постає, — що саме ми захищаємо, і яка мета цього захисту.

Прикладом неадекватного застосування заходів щодо захисту інформації є: Уявіть собі веб-сайт, який містить загальнодоступну інформацію рекламного характеру. Для доступу на цей сайт користувачі мусять проходити попередню процедуру реєстрації з отриманням персонального пароля, який необхідно змінювати щонайменше щотижня. Під час навігації по сайту користувачі отримуватимуть попередження про реєстрацію всіх їхніх дій. Чи буде такий сайт популярним (адже саме це потрібно його власникам)? Усі ці заходи були б цілком прийнятні та навіть необхідні, якби сайт містив, наприклад, конфіденційну корпоративну інформацію.

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, оброблення, зберігання, пошуку та надання користувачам. Ці технології мають ураховувати особливості інформації, які й роблять її цінною, а також давати змогу користувачам різних категорій працювати з інформаційними ресурсами (створювати, знаходити, копіювати, узагальнювати, порівнювати, модифікувати, перетворювати, знищувати тощо).

Тепер визначимо, що може спричинити порушення безпеки інформації та проти чого, власне, застосовують заходи захисту інформації.

Несприятливий вплив — вплив, що призводить до зменшення цінності інформаційних ресурсів.

Загроза — будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку ІКС. Тобто загроза — це будь-який потенційно можливий несприятливий вплив.

Атака — це спроба реалізації загрози. Якщо атака є успішною (здійснено подолання засобів захисту), це називають *проникненням* (рос. — проникновение, англ. — penetration). Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають *компрометацією* (рос. - компрометация, англ. — compromise).

Слід звернути увагу на те, що за комплексного підходу до захисту інформації ми маємо розглядати не лише впливи, спрямовані на інформаційні ресурси, але й будь-які впливи, що можуть завдати шкоди ІКС. Ми вже узагальнили це твердженням про необхідність захисту не самої інформації, а насамперед технології її оброблення.

Уразливість системи — нездатність системи протистояти реалізації певної загрози або ж сукупності загроз.

Вади захисту — сукупність причин, умов і обставин, наявність яких може призвести до порушення нормального функціонування системи або політики безпеки інформації. Здебільшого під вадами захисту розуміють особливості побудови програмних (а іноді й апаратних) засобів захисту, що за певних обставин спричиняють їхню нездатність протистояти загрозам і виконувати свої функції. Тобто вади захисту є окремим випадком уразливості системи.

У літературі іноді використовують інше тлумачення цих термінів, що, як на наш погляд, не є коректним. Наприклад, часто замість терміну *загроза* вживають термін *атака.* Однак потрібно розрізняти атаку, яка є дією, тобто спробою реалізувати певну загрозу, та загрозу, яка робить потенційно можливим здійснення несприятливого впливу. Атака — це здебільшого цілеспрямований вплив, як правило, умисний. Загрози можуть бути випадковими, хоча втрати від цього не стають меншими. Тому захищати інформацію потрібно також від загроз, а не лише від атак.

Порушник — фізична особа (необов'язково користувач системи), яка порушує політику безпеки системи. Іноді використовують термін *зловмисник*, чим наголошують умисність здійсненого ним порушення, тоді як порушник може здійснювати порушення ненавмисно (наприклад, через необережність або недостатню обізнаність).

Часто вживаний термін *хакер* є доволі неоднозначним, тому ми не використовуватимемо його як синонім терміну *порушник.*

Модель [політики] безпеки — абстрактний формалізований чи неформалізований опис політики безпеки. Модель безпеки використовують під час проектування системи для визначення механізмів і алгоритмів захисту, а також під час аналізу захищеності системи для перевірки й доведення коректності та достатності реалізованих механізмів.

Модель загроз — абстрактний формалізований чи неформалізований опис методів і засобів здійснення загроз.

Модель порушника — абстрактний формалізований чи неформалізований опис порушника. Моделі загроз і порушника є вихідною інформацією для розроблення політики безпеки і проектування будь-яких систем захисту.

Захищена комп'ютерна система — комп'ютерна система, що здатна забезпечувати захист оброблюваної інформації від визначених загроз. Цей термін частіше вживають до обчислювальних систем або їхніх складових (програмних продуктів, окремих програмно-апаратних пристроїв). Іноді його застосовують до ІКС, але слід розуміти, що будь-яка сучасна ІКС має бути захищеною (навіть домашній

комп'ютер із одним користувачем). Інакше її використання дуже швидко призведе до втрат інформації.

Спостережність — властивість ІКС, що дає змогу фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів із метою запобігання порушенню політики безпеки і (або) забезпеченню відповідальності за певні дії. Це дуже важлива властивість обчислювальних систем та ІКС, яка досягається реалізацією засобів *реєстрації,* або *аудита* (англ. — audit, auditing).

До можливих загроз безпеці інформації належать:

- стихійні лиха й аварії;
- збої та відмови устаткування;
- наслідки помилок проектування і розроблення компонентів АС;
- помилки персоналу під час експлуатації;
- навмисні дії зловмисників і порушників.

Для побудови моделі загроз використовують різні класифікації загроз безпеці інформації. Наведемо узагальнюючу класифікацію загроз (табл. 1.1).

Таблиця 1.1. Класифікація загроз

Ознака класифікації загроз	Причини, спрямованість, характеристики загроз
Природа виникнення	Природні загрози (загрози, які виникають через виливи на АС та її компоненти об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини). Штучні загрози (загрози, викликані діяльністю людини)
Принцип НСД	Фізичний доступ: ♦ подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів; ♦ розкрадання документів і носіїв інформації; ♦ візуальне перехоплення інформації, виведеної на екрани моніторів і принтери; ♦ підслуховування; ♦ перехоплення електромагнітних випромінювань. Логічний доступ (доступ із використанням засобів комп'ютерної системи)
Мета НСД	Порушення конфіденційності (розкриття інформації). Порушення цілісності (повне або часткове знищення інформації, її спотворення, фальсифікація, викривлення). Порушення доступності (наслідок — відмова в обслуговуванні)
Причини появи вразливостей різних типів	Недоліки політики безпеки. Помилки адміністративного керування. Недоліки алгоритмів захисту. Помилки реалізації алгоритмів захисту
Об'єкт безпосередньої атаки	Політика безпеки АС. Компоненти системи захисту АС. Протоколи взаємодії. Функціональні компоненти АС
Стан кінцевого об'єкта атаки	Зберігання (об'єкт знаходиться на зовнішніх носіях). Оброблення (об'єкт знаходиться в оперативній пам'яті). Передавання (об'єкт просувається через лінію зв'язку)

Спосіб впливу на об'єкт атаки	Безпосередній вплив. Вплив на систему дозволу «Маскарад». Використання наосліп
Спрямованість НСД	Безпосереднє стандартне використання: • слабкостей політики безпеки; • недоліків адміністративного керування. Приховане нестандартне використання: • недокументованих особливостей системи; • прихованих каналів.
Характер впливу	Активний (внесення змін в АС). Пасивний (спостереження)
Режим НСД	За постійної участі людини (в інтерактивному режимі)можливе застосування стандартного ПЗ. Без особистої участі людини (у пакетному режимі) найчастіше для цього застосовують спеціалізоване ПЗ.
Умова початку здійснення впливу	У відповідь на запит від об'єкта, який атакують. Після визначеної події на об'єкті. Безумовна атака
Місцезнаходження джерела НСД	Внутрішньосегментне (джерело знаходиться в локальній мережі). У цьому випадку, як правило, ініціатор атаки — санкціонований користувач. Міжсегментне: • несанкціоноване вторгнення з відкритої мережі в закриту; • порушення обмежень доступу з одного сегмента закритої мережі в інший
Наявність зворотного зв язку	Зі зворотним зв'язком (атакуючий отримує відповідь системи на його вплив) Без зворотного зв'язку (атакуючий не отримує відповіді)
Рівень моделі взаємодії відкритих систем (Open Systems Interconnection, OSI)	Вплив може бути здійснено на таких рівнях: фізичному, канальному, мережному, транспортному, сеансовому, представницькому, прикладному

Таку класифікацію використовують, наприклад, коли потрібно детально проаналізувати загрози, спричинені типовими атаками. Для побудови моделі загроз вона надто громіздка і непрактична. Частіше з цієї класифікації беруть лише перші три характеристики.

Перелік типових загроз безпеці

Розглянемо зручнішу класифікацію, що виглядає, як перелік найтиповіших загроз безпеці. На жаль, це не повний перелік загроз.

1. Природні загрози.
2. Штучні загрози.

2.1. Ненавмисні загрози.

2.1.1. Ненавмисні дії, що призводять до відмови системи.

2.1.2. Неправомірне відключення устаткування чи зміна режимів роботи пристроїв і програм.

2.1.3. Ненавмисне псування носіїв інформації.

2.1.4. Запуск технологічних програм, здатних за некомпетентного використання викликати втрату роботоздатності системи чи незворотпі зміни в ній.

2.1.5. Нелегальне впровадження і використання неврахованих програм.

2.1.6. Ненавмисне зараження вірусом.

2.1.7. Необережні дії, що призводять до розголошення конфіденційної інформації.

2.1.8. Розголошення, втрата атрибутів розмежування доступу.

2.1.9. Проектування архітектури системи з можливостями, що становлять небезпеку для самої системи.

2.1.10. Ігнорування організаційних обмежень.

2.1.11. Входження у систему в обхід засобів захисту.

2.1.12. Некомпетентне використання, настроювання і неправомірне відключення засобів захисту.

2.1.13. Пересилання даних за адресою абонента, яка є хибною.

2.1.14. Введення помилкових даних.

2.1.15. Ненавмисне ушкодження каналів зв'язку.

2.2. Навмисні загрози.

2.2.1. Фізичне руйнування системи.

2.2.2. Вимкнення чи виведення з ладу підсистем забезпечення функціонування.

2.2.3. Дії з дезорганізації функціонування системи.

2.2.4. Вторгнення агентів у оточення персоналу системи.

2.2.5. Вербування персоналу чи окремих користувачів, що мають визначені повноваження.

2.2.6. Застосування пристроїв, що підслуховують, дистанційних фото- та відеозйомок.

2.2.7. Перехоплення побічних електромагнітних, акустичних та інших випромінювань і наведень від пристроїв і каналів зв'язку.

2.2.8. Перехоплення даних, переданих по каналах зв'язку.

2.2.9. Розкрадання носіїв інформації.

2.2.10. Несанкціоноване копіювання носіїв інформації.

2.2.11. Розкрадання і вивчення виробничих відходів.

2.2.12. Зчитування залишкової інформації з оперативної пам'яті та зовнішніх запам'ятовуючих пристроїв.

2.2.13. Незаконне заволодіння паролями.

2.2.14. Несанкціоноване використання терміналів користувачів.

2.2.15. Розкриття шифрів криптографічно захищеної інформації.

2.2.16. Впровадження програмно-апаратних закладок і вірусів.

2.2.17. Незаконне підключення до ліній зв'язку з метою роботи «між рядків».

2.2.18. Незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його повного відключення.

4. Класифікація атак.

Наведемо спрощену класифікацію, яка відображає найбільш типові атаки на розподілені автоматизовані системи. Цю класифікацію було запропоновано Пітером Меллом (Peter Mell).

♦ *Віддалене проникнення*. Атаки, які дають змогу реалізувати віддалене керування комп'ютером через мережу. Приклади програм, що реалізують цей тип атак: NetBus, BackOrifice.

♦ *Локальне проникнення*. Атаки, що призводять до отримання несанкціонованого доступу до вузлів, на яких вони ініційовані. Приклад програми, що реалізує цей тип атак: GetAdmin.

♦ *Віддалена відмова в обслуговуванні*. Атаки, що дають можливість порушити функціонування системи або перенавантажити комп'ютер через мережу (зокрема, через Інтернет). Приклади атак цього типу: Teardrop, trinOO.

♦ *Локальна відмова в обслуговуванні*. Атаки, що дають змогу порушити функціонування системи або перенавантажити комп'ютер, на якому їх ініційовано. Приклади атак цього типу: аплет, який перенавантажує процесор (наприклад, відкривши багато вікон великого розміру), що унеможливлює оброблення запитів інших програм.

♦ *Сканування мережі*. Аналіз топології мережі та активних сервісів, доступних для атаки. Атака може бути здійснена за допомогою службового програмного забезпечення, наприклад за допомогою утиліти nmap.

♦ *Використання сканерів уразливостей*. Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Такі сканери системні адміністратори застосовують як діагностичні інструменти, але їх також можна використовувати для розвідки та здійснення атаки. *Злам паролів*. Для цього використовують програмні засоби, що добирають паролі користувачів. Залежно від надійності системи зберігання паролів, застосовують методи зламу або підбору пароля за словником. Приклади програмних засобів: LOphtCrack для Windows і Crack для UNIX.

♦ *Пасивне прослуховування мережі*. Пасивна атака, спрямована на розкриття конфіденційних даних, зокрема ідентифікаторів і паролів доступу. Приклади засобів: tcpdump, Microsoft Network Monitor, NetXRay, LanExplorer.

Перші чотири класи атак розрізняють переважно за кінцевим результатом (або метою реалізації), а решта — за способом їх здійснення.

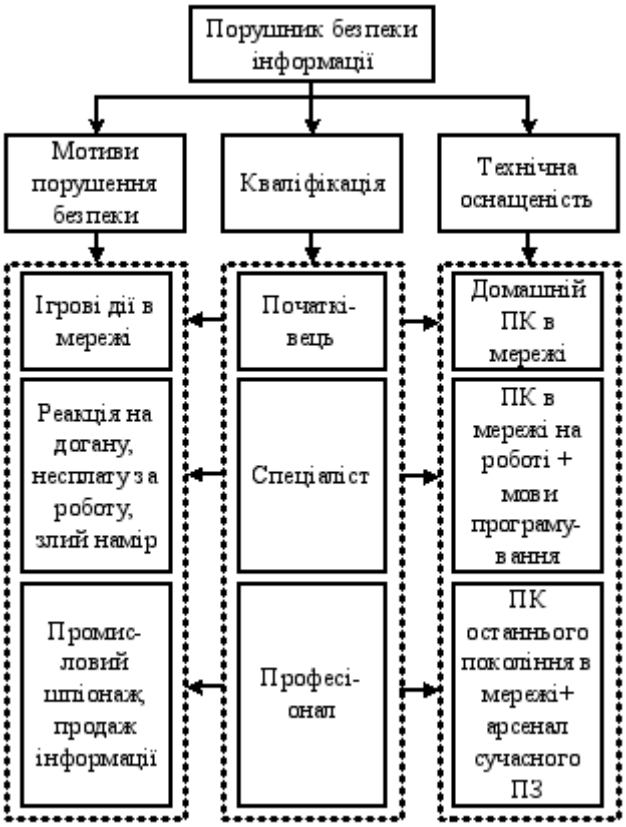
5. Модель порушника

Про хакерів розповідають не лише в засобах масової інформації та Інтернеті, але й в літературі з питань захисту інформації. За своїм історичним походженням і дотепер термін «хакер» застосовують до тих, хто добре розуміється на принципах роботи обчислювальних систем, особливо ПЗ. Ці знання дають їм змогу виявляти вразливості систем. Тобто *хакер* — це той, хто знаходить уразливості системи і знає, як ними можна скористатися.

Є різні думки щодо застосування терміну «хакер». Деякі фахівці в галузі захисту інформації вважають, що справжні хакери — це ті, хто діє виключно в інтересах безпеки інформації. Про виявлені вразливості ці хакери повідомляють лише тих, хто у змозі виправити помилки ПЗ, які й спричинили наявність уразливості. Такі хакери можуть тісно співпрацювати з розробниками ПЗ та експертами з комп'ютерної безпеки.

Модель порушника

Модель порушника — це всебічна структурована характеристика порушника, яку разом із моделлю загроз використовують під час розроблення політики безпеки інформації. Рекомендовано таку структуру моделі порушника.



Категорії порушників:

- внутрішні порушники;
- користувачі;
- інженерний склад;
- співробітники відділів, що супроводжують ПЗ;
- технічний персонал, який обслуговує будинок;
- співробітники служби безпеки;
- керівники;
- зовнішні порушники.

Мета порушника:

- отримання необхідної інформації;
- отримання можливості вносити зміни в інформаційні потоки відповідно до своїх намірів;
- завдання збитків шляхом знищення матеріальних та інформаційних цінностей.

Повноваження порушника в АС:

- запуск фіксованого набору задач (програм);
- створення і запуск власних програмних засобів;
- керування функціонуванням і внесення змін у конфігурацію системи;
- підключення чи змінення конфігурації апаратних засобів.

Технічна оснащеність порушника:

- апаратні засоби;
- програмні засоби;
- спеціальні засоби.

Кваліфікація порушника:

- під час проведення аналізу загроз завжди вважають, що порушник має високу кваліфікацію.