**Лекція 1. Вступна.**

**Вступ.**

**Питання 1. Актуальність проблеми забезпечення безпеки в інформаційних системах.**

**Питання 2. Нормативно-правові аспекти в галузі захисту інформації.**

**Питання 3. Шляхи витоку інформації і несанкціонованого доступу.**

### Питання 4. Архітектура системи безпеки інформації.

**Питання 5. Організаційно-технічні заходи щодо забезпечення безпеки.**

**Вступ**

Нині в Україні, у зв’язку з входженням її у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення компʼютерних і телекомунікаційних технологій. Створені локальні і регіональні обчислювальні мережі; великі території охоплені мережами безпроводового звʼязку; факсовий звʼязок змінився на Вайбер, Телеграм (та ін.) і став доступний для широкого кола користувачів. ІТ-технології та системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У звʼязку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації [1].

**Захист інформації – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння збитку інтересам власника інформації.**

Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виняткове право тієї чи іншої держави. Проте в останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації. Гостра проблема з цього приводу виникла і в Україні. Тому проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різних країн. Внаслідок цього процесу значно зросла потреба у фахівцях із захисту інформації.

І всі Ви, - студенти КБ-41 та КБ-42, після четвертого курсу отримаєте звання Бакалавр зі спеіальності 125 – Кібербезпека.

**Питання 1.**

Інформаційні технології охоплюють методи одержання, обробки, перетворення, зберігання і розподілу інформації. Протягом тривалого часу ці технології розвивалися на мовній і "паперовій" буквено-цифровій основі. У цей час інформаційно-ділова активність людства все більше зміщувалася в сферу кібернетичного простору, який стає реальністю світової спільноти і визначає перехід до "безпаперового, електронного" розвитку інформаційних технологій. Електронний обмін інформацією дешевший, швидший та більш надійніший за "паперовий".

Наприклад, ціна листа з Каліфорнії до Нью-Йорка поштою становить $0,29 (час доставки 2-3 дні), тоді як плата за факс − $1,86, за телекомсистему − $4,56 і, нарешті, за E-mail − всього $0,16, причому час пересилки − не години, а секунди.

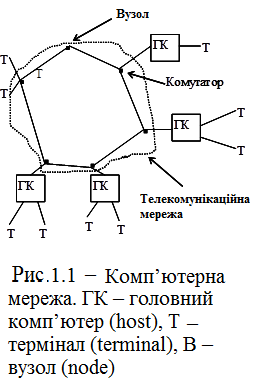
Здійснюється інформаційна "безпаперова" революція. Завдяки виходу в кібернетичний простір зростання інформаційного обміну відбувається за експоненціальним законом.

Інформаційні процеси забезпечення безпеки інформації, що проходять повсюди у світі, висувають на перший план, поряд із завданнями ефективного опрацювання і передачі інформації, − найважливіше завдання. Це пояснюється особливою державною значимістю, розвитком її інформаційних ресурсів, зростанням вартості інформації в умовах ринку, її високою вразливістю і, нерідко, значним збитком у результаті її несанкціонованого використання.

У багатьох країнах порушення безпеки в системах опрацювання і передачі інформації приносять великі втрати. Вони особливо значні в системах телекомунікацій, що обслуговують банківські і торгові потреби. У США, наприклад, збитки від несанкціонованого проникнення в подібні системи оцінюються в десятки мільйонів доларів.

Про ступінь небезпеки електронних злочинів можна судити за тими витратами на засоби захисту, які є припустимими і доцільними. За оцінками спеціалістів США загальні витрати на захист банківського або іншого фінансового застосування можуть скласти усього $510 тис. Проте надійна система захисту значнішої фінансової побудови, що обслуговує до 80 тис. користувачів, коштує не менше $15 млн. Причому, в цю суму входить тільки вартість апаратних і програмних засобів.

Наслідки від несанкціонованого отримання інформації мають різноманітний масштаб: від необразливої прокази до фінансових втрат у великих розмірах. Найбільш вразливими об’єктами, що страждають від несанкціонованого доступу до даних, є системи автоматизованого перерахування коштів. Також частішають випадки розкрадання програм у комп’ютерних мережах, які прийняли характер епідемії: на кожну законну копію програми, що має значне поширення, існує декілька копій, отриманих незаконним шляхом.

Оскільки основний інформаційний обмін заснований на інформаційних технологіях, то важливою умовою стає безпека в комп’ютерних мережах (КМ), порушення якої називають комп’ютерним злочином. Збиток від комп’ютерних злочинів дуже великий (так, крадіжки в Internet за 1 рік призводять збиток $8 млрд.).

Перерахуємо основні загрози для комп’ютерних мереж:

1. Читання інформації (порушення конфіденційності).

2. Порушення цілісності (інтегральності) інформації.

3. Блокування доступу до об’єктів і ресурсів комп’ютерних мереж.

Загрози діляться на пасивні і активні.

До пасивних загроз належать підслуховування (зчитування) інформації та аналіз трафіка (ідентифікація користувачів і визначення інтенсивності інформаційного обміну).

До активних загроз належать модифікація даних, створення фальшивих даних під чужим іменем, введення вірусів і програмних закладок, блокування доступу до ресурсів комп’ютерних мереж.

**Основні можливі місця вторгнення в комп’ютерну мережу показані на рис.1.1. Це:**

**1. Термінали (монітори, принтери, клавіатура, пульти, телефонні апарати).**

**2. Комутатори у вузлах КМ.**

**3. Лінії зв’язку (модеми, підсилювачі, ретранслятори).**

**4. Комп’ютерні процесори.**

**5. Файли на різноманітних носіях.**

**6. Додаткові плати, карти.**

**7. Пластикові карти.**

**8. Бази даних.**

Зауважимо, що протяжність КМ призводить до її значної вразливості і до труднощів відслідковування комп’ютерних злочинів.

Комп’ютерні злочини можуть мати місце в органах державного і регіонального управління, на оборонних і інших державних підприємствах, у комерційних та промислових структурах. Вони можуть скоюватися приватними особами, у тому числі клієнтами банків. Основними групами правопорушників є: хакери (hackers), крейкери (creakers), терористи й екстремісти, а також комерційні підприємства, що ведуть промислове шпигунство. Ціллю захисту інформації є запобігання приведеним до виконання перерахованим вище загрозам.

В обчислювальних машинах є велике число лазівок для несанкціонованого доступу до інформації. Ніякий окремо взятий спосіб захисту не може забезпечити адекватну безпеку. Надійний захист може бути гарантований лише при створенні механізму комплексного забезпечення безпеки: як засобів опрацювання інформації, так і каналів звʼязку [10].

**Комплексна система захисту інформації (надалі, - КСЗІ)**– сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

**Організаційні заходи** є обов'язковою складовою побудови будь-якої КСЗІ.

**Інженерно-технічні** заходи здійснюються в міру необхідності.

Термін та визначення **«інженерні засоби»** було введено російськими фахівцями галузі інформаційної безпеки.

**Технічні засоби** представляють собою електричні, механічні, електромеханічні або електронні пристрої. Вся сукупність технічних засобів ділиться на фізичні й апаратні.

**Фізичні засоби** реалізуються у вигляді автономних пристроїв та систем, вони виконують функції загального захисту обʼєктів, на яких опрацьовується інформація. До них ставляться, наприклад, пристрої захисту територій і будинків, замки на дверях приміщень, де розміщена апаратура, грати на вікнах, електронно-механічне устаткування охоронної сигнализації.

Під **апаратними технічними (апаратно-технічними) засобами** прийнято розуміти пристрої, що вмонтовуються безпосередньо в обчислювальну техніку, у телекомунікаційну апаратуру, або пристрої, що працюють з подібною апаратурою за стандартним інтерфейсом. З найбільш відомих апаратних засобів можна виділити схеми контролю інформації з парності, схеми захисту масивів памʼяті за ключем та ін.

**Програмні засоби** − програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

**Організаційні засоби** захисту представляють собою організаційно-технічні й організаційно-правові заходи, що здійснюються в процесі створення й експлуатації апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їхнього життєвого циклу (будівництво приміщень, проектування системи, монтаж і налагодження устаткування, перевірка і експлуатація).

**Морально-етичні засоби** захисту реалізуються у вигляді всіляких норм, що склалися традиційно в даній країні або товаристві. Ці норми здебільшого не є обовʼязковими як законодавчі акти, проте їхнє недотримання веде, звичайно, до втрати авторитету і престижу співробітника.

**Законодавчі засоби** захисту визначаються законодавчими актами країни, які регламентують правила використання, опрацювання і передачі інформації обмеженого доступу і встановлюють міру відповідальності за порушення цих правил.

Необхідно також зазначити, що всі розглянуті засоби захисту діляться на формальні, які виконують захисні функції строго за заздалегідь передбаченими процедурами без особистої участі людини, і неформальні, обумовлені цілеспрямованою діяльністю людини або регламентуючою цієї діяльності.

**Питання 2.**

**Нормативно-правове забезпечення організації і здійснення заходів щодо захисту інформації являє собою сукупність законів, нормативних актів і правил, що регламентують як загальну організацію робіт, так і створення та функціонування конкретних систем захисту інформації.**

В даний час в Україні, як і в інших країнах, нормативно-правова база захисту інформації знаходиться на стадії формування.

При побудові правової бази системи безпеки інформації в Україні розвʼязується ряд завдань.

Розробка в якості правової основи системи забезпечення безпеки інформації базового закону, що регламентує відношення і розмежування сфери повноважень усіх учасників інформаційних взаємозвʼязків, а також визначальні державні органи, що забезпечують інформаційну безпеку і засоби контролю з боку держави за розмежуванням доступу до інформації.

**Розробка законодавчих актів і правових норм**, що всебічно охоплюють усі проблеми захисту інформації, і підходів, що відображають специфіку забезпечення безпеки інформації в різноманітних сферах діяльності держави і товариства – це дуже важливе завдання, як і регламентація рівнів безпеки інформації та адекватних їм методів і засобів захисту.

Однією з найбільш важливих складових частин правового забезпечення системи безпеки інформації є **стандартизація і сертифікація**, що повинні вирішувати наступні завдання:

1 - Створення пакета основних стандартів організаційно-методичного і термінологічного забезпечення системи захисту інформації.

2 - Стандартизація вимог із захисту інформації в засобах обчислювальної техніки в автоматизованих системах, інформаційних мережах і засобах телекомунікації.

3 - Нормативне і метрологічне забезпечення сертифікації й атестації технічних засобів захисту інформації і контролю їхньої ефективності.

**Закон України "Про інформацію**" [1] встановлює загальні правові основи одержання, використання, поширення і збереження інформації. Відповідно до цього закону:

**Інформація – це документовані або привселюдно оголошені відомості про події і явища, що відбуваються в товаристві, державі або навколишньому природньому середовищі.**

Закон закріплює право власності на інформацію у всіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації і забезпечує її охорону, захищає особистість і товариство від помилкової інформації. Чинність закону поширюється на інформаційні відносини, що виникають у всіх сферах життя і діяльності товариства і держави при одержанні, використанні, поширенні і збереженні інформації.

Субʼєктами інформаційних відносин є громадяни України, юридичні особи, держава Україна, а також інші держави, їхні громадяни і юридичні особи, міжнародні організації й особи без громадянства. З метою задоволення потреби в інформаційній діяльності створюються інформаційні служби, системи, мережі, бази і банки даних. Закон передбачає створення загальної системи охорони інформації.

**Відповідно до закону основними видами інформації є:**

* **статистична інформація;**
* **масова інформація;**
* **інформація про діяльність державних органів влади й органів місцевого та регіонального самоврядування;**
* **правова інформація;**
* **інформація про особистість;**
* **інформація довідково-енциклопедичного характеру;**
* **соціологічна інформація.**

Категорії інформації і режими доступу до неї визначаються такими статтями Закону [1].

Стаття 28. Режим доступу до інформації:

**Режим доступу до інформації − це передбачений правовими нормами порядок одержання, використання, поширення і збереження інформації**.

За режимом доступу інформація поділяється на відкриту та інформацію з обмеженим доступом. Держава здійснює контроль за режимом доступу до інформації.

Завдання контролю за режимом доступу до інформації полягає в забезпеченні дотримання вимог законодавства про інформацію всіма державними органами, підприємствами й організаціями і недопустимості необгрунтованого ставлення до категорії інформації з обмеженим доступом.

Державний контроль за дотриманням установленого режиму здійснюється спеціальними органами, що визначаються Верховною Радою України і Кабінетом Міністрів України.

У порядку контролю Верховна Рада України може вимагати від урядових структур, міністерств та відомств звіти, що містять дані про їхню діяльність з забезпечення інформацією зацікавлених осіб (кількість випадків відмови в наданні доступу до інформації із вказівкою мотивів таких відмов; кількість і обгрунтування застосування режиму обмеженого доступу до окремих видів інформації; кількість скарг на неправомірні дії посадових осіб, що відмовили в доступі до інформації, вжиті до них заходи і т.п.).

**Стаття 30. Інформація з обмеженим доступом**

**Інформація з обмеженим доступом за своїм правовим режимом ділиться на конфіденційну і таємну.**

**Конфіденційна інформація − це дані, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і що поширюються за їхнім бажанням відповідно до передбачених ними умов**.

Громадяни, юридичні особи, що володіють інформацією фахового, ділового, виробничого, банківського, комерційного й іншого характеру, отриманою за власні засоби, або яка є предметом їх фахового, ділового, виробничого, банківського, комерційного й іншого інтересу і не порушують передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи приналежність її до категорії конфіденційної, і встановлюють для неї систему (засоби) захисту.

**Виняток** становить інформація комерційного і банківського характеру, а також інформація, правовий режим якої встановлений Верховною Радою України за предʼявленням Кабінету Міністрів України (із питань статистики, екології, банківських операцій, податків і т.п.), та інформація, утаювання якої являє загрозу життю і здоровʼю людей.

**До таємної інформації належить інформація, яка містить дані, що складають державну й іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, товариству і державі**. Віднесення інформації до категорії таємних даних, що становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про інформацію. Порядок обігу таємної інформації і її захист визначається відповідними державними органами за умови дотримання вимог, установлених чинним законодавством.

Порядок і терміни обнародування таємної інформації визначаються відповідним законом.

Стаття 53. Інформаційний суверенітет.

**Основою інформаційного суверенітету України є національні інформаційні ресурси.**

До інформаційних ресурсів України належать вся приналежна їй інформація, незалежно від її отримання, форм, часу і місця створення. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Стаття 54. Гарантії інформаційного суверенітету України.

Інформаційний суверенітет України забезпечується: винятковим правом власності України на інформаційні ресурси, що формуються за рахунок засобів державного бюджету, створенням національних систем інформації, встановленням режиму доступу інших держав до інформаційних ресурсів України, використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

**Метою Закону України "*Про захист інформації в автоматизованих системах*" [2]** є встановлення основ регулювання правових відносин про захист інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію і права доступу до неї, права власника інформації на її захист, а також установленого чинним законодавством обмеження на доступ до інформації.

Чинність цього Закону поширюється на будь-яку інформацію, оброблювану в автоматизованих системах. У Законі основні терміни вживаються в такому значенні.

- **Автоматизована система (АС)** – система, що здійснює автоматизоване опрацювання даних, до складу якої входять технічні засоби опрацювання (засоби обчислювальної техніки і звʼязку), а також методи, процедури і програмне забезпечення.

- **Інформація в АС** – сукупність усіх даних і програм, що використовуються в АС незалежно від засобу їх фізичного та логічного уявлення.

- **Опрацювання інформації** – сукупність операцій (збір, введення, запис, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних.

- **Захист інформації** – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню збитку інтересам власника інформації або АС і осіб, що користуються інформацією.

- **Несанкціонований доступ до** **інформації** – доступ, що здійснюється із порушенням встановлених в АС правил розмежування доступу.

- **Розпорядник АС** – фізична або юридична особа, що має право розпоряджатися АС за згодою з її власником або за його дорученням.

- **Користувач АС** – фізична або юридична особа, що має право використання АС за згодою розпорядника АС.

- **Порушник** – фізична або юридична особа, яка навмисно або ненавмисно здійснює неправомірні дії стосовно АС і інформації в ній.

- **Витік інформації** – результат дій порушника, внаслідок яких інформація стає відомою (доступною) субʼєктам, що не мають права доступу до неї.

- **Втрата інформації** – дія, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, що мають право власності на неї в повному або обмеженому обсязі.

- **Підробка інформації** − навмисні дії, що ведуть до перекручування інформації, яка повинна опрацьовуватися або зберігатися в АС.

- **Блокування** інформації − це дії, наслідком яких є припинення доступу до інформації.

**Відповідно до Закону обʼєктами захисту є інформація, що обробляється в АС, права власників цієї інформації і власників АС, права користувача. Захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством.**

**Доступ до інформації, що зберігається, опрацьовується і передається в АС, здійснюється лише відповідно до правил розмежування доступу, установлених власником інформації або уповноваженою ним особою.** Без дозволу власника доступ до інформації, що опрацьовується в АС, здійснюється лише у випадках, передбачених чинним законодавством.

**Власник АС повинен** забезпечити захист інформації відповідно до вимог і правил, що обумовлюються угодою з власником інформації або уповноваженою ним особою, і зобовʼязаний повідомити йому про всі факти порушення її захисту.

**Власник інформації має право** здійснювати контроль за дотриманням вимог щодо захисту інформації і забороняти або припиняти опрацювання інформації у випадку порушення цих вимог.

Власник інформації та уповноважені ним на те особи визначають користувачів приналежної йому інформації і встановлюють їхні повноваження.

Власник АС дає користувачам можливість доступу до інформації, оброблюваної в АС, відповідно до повноважень, наданих власником інформації.

Розпорядник АС інформує власника інформації про технічні можливості захисту інформації в його АС, типові правила, встановлені для персоналу АС.

Приведемо перелік найбільш важливих статей Закону, що стосуються умов опрацювання і заходів для забезпечення захисту інформації.

**Стаття 10. Забезпечення захисту інформації в АС.**

**Захист інформації в АС забезпечується шляхом:**

**- дотримання субʼєктами правових відносин, норм, вимог і правил організаційного та технічного характеру із захисту оброблюваної інформації; використання засобів обчислювальної техніки, програмного забезпечення, засобів звʼязку й АС в цілому, засобів захисту інформації, що відповідають установленим вимогам із захисту інформації (мають відповідний сертифікат);**

**- перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів звʼязку й АС в цілому установленим вимогам із захисту інформації (сертифікація засобів обчислювальної техніки, засобів звʼязку та АС);**

**- здійснення контролю щодо захисту інформації.**

Стаття 11. Встановлення вимог і правил захисту інформації.

Вимоги і правила із захисту інформації, що є власністю держави, або інформації, захист якої гарантується державою, встановлюються державним органом, уповноваженим Кабінетом Міністрів України. Ці вимоги і правила є обовʼязковими для власників АС, де така інформація опрацьовується, і носить рекомендаційний характер для інших субʼєктів права власності на інформацію.

Стаття 12. Умови опрацювання інформації.

Інформація, що є власністю держави, або інформація, захист якої гарантується державою, повинна опрацьовуватися в АС, що має відповідний сертифікат (атестат) захищеності, в порядку, обумовленому уповноваженим Кабінетом Міністрів України органом.

У процесі сертифікації (атестації) цих АС здійснюються також перевірка, сертифікація (атестація) розроблених засобів захисту інформації.

Інформація, що є власністю інших субʼєктів, може опрацьовуватися в зазначених АС за розпорядженням власника інформації. Власник інформації може звернутися в органи сертифікації з клопотанням про проведення аналізу можливостей АС для належного захисту його інформації й одержання відповідних консультацій.

Стаття 13. Політика в області захисту інформації.

Політика в області захисту інформації в АС визначається Верховною Радою України.

Стаття 14. Державне управління захистом інформації в АС.

Уповноважений Кабінетом Міністрів України орган здійснює керівництво захистом інформації шляхом:

- проведення єдиної технічної політики щодо захисту інформації;

- розробки концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій щодо захисту інформації в АС;

- затвердження порядку організації, функціонування і контролю за виконанням заходів, спрямованих на захист оброблюваної в АС інформації, що є власністю держави, а також рекомендацій із захисту інформації власності юридичних і фізичних осіб;

- організації іспитів і сертифікації засобів захисту інформації в АС, у якій здійснюється опрацювання інформації, що є власністю держави;

- створення відповідних структур для захисту інформації в АС;

- проведення атестації сертифікаційних (іспитових) органів, центрів і лабораторій, видача ліцензії на право проведення сервісних робіт в області захисту інформації в АС;

- дійснення контролю захищеності оброблюваної в АС інформації, що є власністю держави;

- визначення порядку доступу осіб і організацій іноземних держав до інформації в АС, що є власністю держави, або до інформації власності фізичних і юридичних осіб, щодо поширення і використання якої державою встановлені обмеження.

Міністерства, відомства й інші центральні органи державної влади забезпечують вирішення питань захисту інформації в АС у межах своїх повноважень.

**Стаття 15. Служби захисту інформації в АС.**

**У державних установах і організаціях можуть створюватися підрозділи, служби, що організовують роботу, повʼязану з захистом інформації, підтримкою рівня захисту інформації в АС, і відповідають за ефективність захисту інформації відповідно до вимог даного Закону**.

Стаття 20. Забезпечення інформаційних прав України.

Фізичні і юридичні особи в Україні на підставі Закону України "Про інформацію" можуть встановлювати взаємозвʼязок з АС інших держав з метою опрацювання, обміну, продажу, покупки відкритої інформації. Такі взаємозвʼязки повинні виключати можливість несанкціонованого доступу з боку інших держав або їхніх представників резидентів чи осіб без громадянства до інформації, наявної в АС України, незалежно від форм власності і підпорядкування, у відношенні якої встановлені вимоги нерозповсюдження її за межі України без спеціального дозволу.

Іноземні держави, іноземні фізичні і юридичні особи можуть виступати власниками АС в Україні, власниками інформації, що поширюється й опрацьовується в АС України, або організовувати спільні з українськими юридичними і фізичними особами підприємства з метою створення АС України, обміну інформацією між АС України й АС інших держав. Окремі види такої діяльності здійснюються на підставі спеціального дозволу (ліцензії), що видається уповноваженим на це органом.

**Питання 3.**

Несанкціонований доступ до телекомунікаційних систем призводить до значних матеріальних втрат. Для успішної боротьби з порушеннями інформаційної безпеки користувач повинен знати всі канали витоку інформації.

Аналіз показує, що **шляхи несанкціонованого одержання інформації дуже різноманітні і багато численні:**

**1) несанкціоноване підключення до апаратури і ліній зв’язку;**

**2) перехоплення електромагнітних випромінювань;**

**3) примусове електромагнітне опромінення (підсвічування) ліній зв’язку з метою одержання паразитної модуляції несучої частоти;**

**4) застосування пристроїв, що підслухують, (закладань);**

**5) перехоплення акустичних випромінювань;**

**6) дистанційне фотографування;**

**7) розкрадання носіїв інформації і виробничих відходів;**

**8) зчитування даних у масивах інших користувачів;**

**9) читання залишкової інформації в памʼяті системи після виконання санкціонованих запитів;**

**10) копіювання носіїв інформації з подоланням засобів захисту;**

**11) маскування під зареєстрованого користувача;**

**12) використання програмних пасток,**

**13) використання недоліків мов програмування й операційних систем;**

**14) вмикання в бібліотеки програм спеціальних блоків типу "троянський кінь";**

**15) злочинне виведення з ладу механізмів захисту;**

**16) впровадження і використання компʼютерних вірусів.**

**Близьким по характеру є і *перелік загроз* *безпеки* інформації.**

Перехоплення даних огляд даних несанкціонованим користувачем. Ця загроза виявляється в можливості порушника безпосередньо підключатися до лінії звʼязку для знімання переданої інформації або одержання інформації на відстані з використанням побічного електромагнітного випромінювання при передачі інформації з ліній звʼязку.

Аналіз трафіка та огляд інформації, що стосується звʼязку між користувачами (наприклад, наявність/відсутність, частота, напрямок, послідовність, тип, обсяг обміну і т.д.). Навіть якщо підслуховуючий не може визначити фактичного отримання повідомлень, він може одержати деякий обсяг інформації, виходячи з характеру потоку інформації (наприклад, беззупинний, пакетний, або відсутність інформації).

Зміна потоку повідомлень внесення не знаходить перекручувань у повідомленні, видалення повідомлень або порушення загального порядку повідомлень у потоці.

Відмова користувача від повідомлення, заперечення відправником свого авторства в предʼявленому йому одержувачем повідомленні або заперечення одержувачем факту одержання ним повідомлення.

Маскарад – це прагнення порушника видати себе за деякого іншого користувача з метою одержання доступу до додаткової інформації, одержання додаткових привілеїв або навʼязування іншому користувачу помилкової інформації.

Порушення звʼязку, недопущення звʼязку або затримка термінових повідомлень.

Аналізуючи шлях несанкціонованого доступу, можна зробити припущення, що для побудови сучасних систем охоронних сигналізацій обовʼязковим буде наявність радіоканалу, а також використання широкосмугових сигналів (ШСС) для безпечної передачі даних по цьому каналу.

**Питання 4.**

Необхідність забезпечення безпеки і вимоги сумісності різноманітних служб існуючих і розроблювальних інформаційно-обчислювальних мереж спонукали до визначення напрямків у діяльності Міжнародної організації із стандартизації і Міжнародної спілки електрозвʼязку. Концепція архітектури безпеки орієнтується на застосуванні в мережах, що використовують міжнародні стандарти, і цілком відповідає еталонній моделі взаємозвʼязку відкритих систем. Забезпечення безпеки інформації при її передачі здійснюється спеціальним підрозділом, що включає в себе ряд служб, кожна з яких вирішує завдання захисту інформації від визначеної загрози (сукупності загроз).

**Загалом випадку в систему забезпечення безпеки інформації можуть бути включені:**

**1) Служба таємності даних може бути використана для захисту переданих даних від витоку інформації, що утримується в них, і від можливості проведення аналізу інтенсивності потоків даних між користувачами.**

**2) Служба аутентифікації призначена для підтвердження того, що в даний момент звʼязку користувач є дійсно тим користувачем, за якого він себе видає.**

**3) Служба цілісності даних забезпечує доказ цілісності даних у процесі їхньої передачі, тобто забезпечує захист переданих повідомлень від випадкових і навмисних впливів, спрямованих на зміну переданих повідомлень, затримку і знищення повідомлень або перевпорядкування повідомлень.**

**4) Служба керування доступом забезпечує захист від несанкціонованого доступу до інформації, що утримується у віддалених банках даних, або від несанкціонованого використання мережі.**

**5) Служба цілісності інформації забезпечує доказ цілісності повідомлення, прийнятого від відповідного джерела, що знаходиться на збереженні, наприклад, у терміналі-приймачі, і яке може бути перевірене в будь-який момент часу арбітром (третьою стороною).**

**6) Служба доставки забезпечує захист від спроб зловмисника порушити звʼязок або затримати передачу повідомлення на час, що перевищує час цінності переданої в повідомленні інформації; ця служба безпосередньо повʼязана з процесами передачі інформації в мережах звʼязку.**

Механізм шифрування може забезпечувати конфіденціальність або переданих даних, або інформації про параметри трафіка і може бути використаний у деяких інших механізмах безпеки або доповнювати їх. Існування механізму шифрування припускає використання, як правило, механізму керування ключами.

У механізмі аутентифікації основна увага приділяється методам передачі в мережі інформації спеціального характеру (полів аутентифікаторів, контрольних сум і т.д.). У випадку односторонньої або взаємної аутентифікації забезпечується процес перевірки істинності користувачів (передавача і приймача повідомлень), що гарантує запобігання зʼєднання з логічним обʼєктом, утвореним зловмисником.

Механізм забезпечення цілісності даних припускає введення в кожне повідомлення деякої додаткової інформації, що є функцією від змісту повідомлення. У рекомендаціях методів охоронних систем розглядаються методи забезпечення цілісності двох типів:

- перші забезпечують цілісність єдиного блока даних;

- другі − потоку блоків даних або окремих полів цих блоків.

Ці методи застосовуються як при передачі даних за віртуальним зʼєднанням, так і при використанні датаграмної передачі. У першому випадку гарантується усунення повторів, вставок або модифікацій даних за допомогою спеціальної нумерації блоків або введенням міток часу. У датаграмному режимі мітки часу можуть забезпечити тільки обмежений захист цілісності послідовності блоків даних і запобігти переадресації окремих блоків.

**Таблиця 1.1. Служби і процедури захисту**

| **Найменування служби** | **Номер служби** | **Процедура захисту** | **Номер рівня** |
| --- | --- | --- | --- |
| А у т е н т и ф і к а ц і я: | | | |
| Однорівневих обʼєктів | 1 | Шифрування, цифровий підпис, забезпечення аутентифікації. | 3, 4,7 |
| Джерела даних | 2 | Шифрування, цифровий підпис | 3,4,7 |
| Контроль доступу | 3 | Керування доступом | 3,4,7 |
| З а с е к р е ч у в а н н я: | | | |
| Зʼєднання | 4 | Шифрування | 14, 6 |
| Керування маршрутом | 7 |
| В режимі без з'єднання | 5 | Шифрування | 24, 6 |
| Керування маршрутом | 7 |
| Вибіркових полів | 6 | Шифрування | 6,7 |
| Потоку даних | 7 | Шифрування | 1,6 |
| Заповнення потоку | 3,7 |
| Керування маршрутом | 3 |
| З а б е з п е ч е н н я ц і л о с н о с т і: | | | |
| Зʼєднання з відновленням | 8 | Шифрування, забезпечення цілосності даних | 4,7 |
| Зʼєднання без відновлення | 9 | Шифрування, забезпечення цілосності даних | 3,4,7 |
| Вибіркових полів даних | 10 | Шифрування, забезпечення цілосності даних | 7 |
| Без встановлення зʼєднання | 11 | Шифрування | 3,4,7 |
| Цифровий підпис | 4 |
| Забезпечення цілосності даних | 3,4,7 |
| Вибіркових полів без зʼєднання | 12 | Шифрування | 7 |
| Цифровий підпис | 4,7 |
| Забезпечення цілосності даних | 7 |
| І н ф о р м у в а н н я: | | | |
| Про відправку | 13 | Цифровий підпис, забезпечення цілосності даних, підтвердження характеристик даних | 7 |
| Про доставку | 14 | Цифровий підпис, забезпечення цілосності даних, підтвердження характеристик даних | 7 |

**Механізм цифрового електронного підпису, що регламентує один із процесів аутентифікації користувачів і повідомлень, використовується для підтвердження істинності змісту повідомлення і посвідчення того факту, що воно відправлено тим абонентом, який зазначений в заголовку якості джерела даних. Цифровий підпис також необхідний для запобігання можливості відмови передавача від видачі якогось повідомлення, а приймача − від його прийому.**

Процес підписання блоку даних використовує інформацію, що є інформацією приватного використання (тобто унікальною і конфіденційною). Цей процес припускає або шифрування блоку даних, або одержання криптографічного контрольного значення блоку даних із використанням приватної інформації користувача, що підписав у якості ключа шифрування приватного користування. Таким чином, після перевірки підпису в наступній третій особі (наприклад, арбітру) у будь-який час може бути доведено, що підпис міг виконати тільки єдиний тримач секретної (приватної) інформації.

Механізми контролю доступу можуть використовувати аутентифікаційну ідентифікацію обʼєкта або інформацію обʼєкта (наприклад, приналежність до відомої множини обʼєктів), або можливості цього обʼєкта для встановлення і застосування прав доступу до цього обʼєкта. Якщо обʼєкт робить спробу використовувати несанкціонований ресурс або санкціонований ресурс із неправильним типом доступу, то функція контролю доступу буде відхиляти цю спробу і може повідомити про цю спробу для ініціювання аварійного сигналу і (або) реєстрації його як частини даних перевірки безпеки. Механізми контролю доступу можуть використовуватися на будь-якому кінці зʼєднання і (або) у будь-якому проміжному вузлі.

Механізм підстановки трафіка, названого також механізмом заповнення потоку, використовується для реалізації служби засекречування потоку даних. Він грунтуються на генерації фіктивних блоків, їх шифрування й організації передачі по каналах звʼязку. Таким чином нейтралізується можливість одержання інформації про мережу і абоненти, що обслуговуються нею, за допомогою спостереження за зовнішніми характеристиками потоків, що циркулюють по каналах звʼязку.

**Питання 5.**

### 

**Безпека інформації в системах телекомунікації забезпечується застосуванням комплексу прийомів, що можна класифікувати в такий спосіб:**

**- організація охорони помешкань, у тому числі із застосуванням систем радіосигналізації; забезпечення безпеки компʼютерних систем програмними й апаратними засобами;**

**- періодичне тестування помешкань методами нелінійної радіолокації;**

**- забезпечення захищеності від прослуховування засобів мобільного радіозвʼязку;**

**- забезпечення акустичної безпеки помешкань і персоналу;**

**- криптографічні заходи.**

Нижче зупинимося на *аналізі* *організаційно-технічних прийомів*.

Організаційні заходи включають активне вивчення і використання нормативно-законодавчої бази із забезпечення безпеки в інформаційних і телекомунікаційних системах, добір персоналу, що допускається до обробки конфіденційної інформації, організацію збереження і доступу до документів, організацію контрольно-пропускного й охоронного режиму, виключення впливу стихійних лих на безпеку збереженої й опрацьовуваної інформації і т.п.

**На початковій стадії організації робіт:**

* встановлюється наявність конфіденційної інформації в системі, оцінюється рівень її конфіденційності й обсяг;
* оцінюється можливість використання наявних на ринку сертифікаційних засобів захисту, виходячи з режиму обробки і передачі інформації в системі, типу системи, складу основних технічних засобів і т.д.;
* визначається ступінь участі персоналу, функціональних і виробничих служб у процесі опрацювання і передачі інформації, характер їхньої взаємодії між собою і зі службою забезпечення безпеки;
* визначається план заходів щодо забезпечення безпеки.

Важливе місце в системі організації робіт із забезпеченням безпеки інформації на підприємствах повинні займати служби захисту інформації, основним завданням яких є організація робіт з виявлення можливостей і запобігання витоку інформації, методичне керівництво й участь у розробці вимог із захисту інформації від несанкціонованого доступу, аналітичного обґрунтування необхідності захисту інформації, узгодження вибору програмно-технічних засобів і систем захисту.

Для ефективної і надійної роботи системи забезпечення безпеки інформації необхідно правильно організувати дозвільну процедуру доступу користувачів до інформації, тобто надати користувачам право працювати з тією інформацією, що необхідна їм для виконання своїх функціональних обов’язків, установити їх повноваження для доступу до інформації.

Серед організаційних заходів щодо забезпечення безпеки інформації важливе місце займає охорона обʼєкта, на якому розміщена захисна система (територія, будинки, помешкання, сховища інформаційних носіїв і т.д.), шляхом встановлення відповідних постів технічних засобів охорони, що запобігають розкраданню інформаційних носіїв, а також несанкціонованому доступу до апаратури і каналів звʼязку.

Системи охоронної сигналізації можна умовно віднести до одного з двох основних видів: автономні і централізовані. В свою чергу, автономні системи охоронної сигналізації можуть подавати сигнал тривоги на місці установки або передавати повідомлення на віддалений пульт. Централізовані системи охоронної сигналізації зазвичай припускають наявність пульта, на якому відображається стан обʼєктів, що охороняються, і чергового персоналу.

Найбільше поширення серед відомчих систем охоронної сигналізації раніше одержали системи, у яких апаратура аналізу стану обʼєктів, що охороняються, зосереджена на центральному пульті, а звʼязок із розташованими в охоронних помешканнях датчиками здійснюється по виділених провідних лініях. У загально громадських системах сигналізації (позавідомча охорона) апаратура аналізу стану обʼєкта знаходиться в помешканні, що охороняється, а звʼязок її з апаратурою центрального пульта здійснюється по лініях телефонного звʼязку.

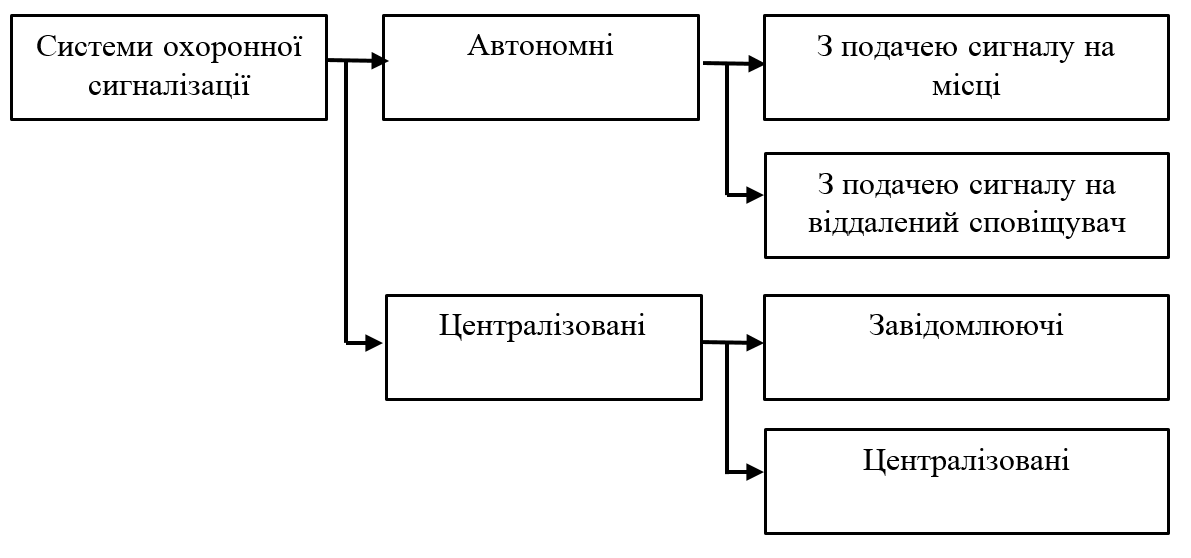


Рис. 1.2 – Види системної охоронної сигналізації

Системам охоронної сигналізації властиві такі недоліки:

1. Наявність провідного звʼязку між помешканням, що охороняється, і центральним пультом, а також досить прості сигнали в лініях звʼязку, що залишають можливість підключення до цих ліній з метою злочинного порушення правильного функціонування системи.

2. Обмеження за числом абонентів у звʼязку з концепцією апаратного рішення.

3. Якість телефонних і виділених ліній звʼязку недостатньо висока для забезпечення високої надійності роботи системи. Підтримка їх у робочому стані повʼязана з додатковими поточними витратами.

4. Підключення нових обʼєктів потребує наявності телефонної або прокладки виділеної лінії звʼязку, що збільшує розмір початкових витрат і обмежує можливість розширення системи.

5. В рамках існуючих систем неможливе без істотних капітальних вкладень підключення віддалених окремо розташованих обʼєктів.

Крім очевидних недоліків першого варіанта, практика їх застосування в останні роки виявила такі особливості, як конфліктність із факсами, що залишаються на ніч в автоматичному режимі, та автовідповідачами телефонів

Основною характерною рисою діяльності підприємства, повʼязаного з обробкою і передачею інформації, що підлягає захисту, є функціонування системи захисту інформації як комплексу програмно-технічних засобів і організаційних рішень, які передбачають наступне:

* урахування, збереження і видачу користувачам інформаційних носіїв, паролів, ключів;
* ведення службової документації служби захисту інформації (генерацію паролів, ключів, супровід правил розмежування доступу);
* оперативний контроль за функціонуванням служби захисту інформації;
* контроль за ходом технологічного процесу опрацювання і передачі інформації шляхом реєстрації аналізу дій користувачів, сигналізації про небезпечні події.

Для надійного захисту території обʼєктів сучасний комплекс повинен містити в собі такі основні компоненти:

* механічну систему захисту;
* пристрій оповіщення про спроби вторгнення;
* оптичну (телевізійну) систему розпізнання порушників;
* центральний пост охорони, що здійснює збір, аналіз, реєстрацію й представлення повідомлень, які надходять, а також керування периферійними пристроями (брамою, загородженнями і ін);
* персонал охорони (патрулі, чергові на центральному посту).

У якості механічних засобів захисту використовуються: цегельні або камʼяні стіни, рови, огорожі, спеціальні дротові огородження, штахети і інше. Ці перешкоди можуть мати багаторядну систему для збільшення часу опору порушнику.

Сповіщення про вторгнення на територію, що охороняється, здійснюється за допомогою різноманітних датчиків. У системах захисту периметру території без огорожі використовують мікрохвильові, інфрачервоні, ємнісні й електричні датчики.

Мікрохвильові системи грунтуються на контролі інтенсивності надвисокочастотного випромінювання, спрямованого від передавача, що сприймається приймачем. Спрацьовування сигналізації відбувається при перериванні цього спрямованого випромінювання. Помилкові вмикання сигналізації (помилкова тривога) можуть бути обумовлені переміщенням у контрольованій зоні тварини, впливом рослинності, атмосферних опадів, пересуванням транспортних засобів, а також впливом сторонніх передавачів.

У інфрачервоних системах між передавачем і приймачем контролюється інтенсивність монохроматичного світлового випромінювання в невидимій інфрачервоній області. Спрацьовування сигналізації відбувається при перериванні одного або декількох світлових променів. Помилкові вмикання сигналізації можуть бути обумовлені переміщенням у контрольованій зоні тварин, сильним туманом або снігопадом.

Принцип дії ємнісної системи оповіщення ґрунтується на формуванні електростатичного поля між паралельно розташованими передаючими і сприймаючими дротовими елементами спеціального огородження. Спрацьовування сигналізації відбувається при реєстрації визначеної зміни електростатичного поля, що має місце при наближенні людини до елементів огородження. Помилкові вмикання сигналізації обумовлені переміщенням тварини, впливом рослинності, зледенінням елементів огородження, атмосферними впливами або забрудненням ізоляторів.

Електричні системи оповіщення базуються на використанні спеціального огородження з дротового матеріалу, що проводить струм. Критерієм спрацьовування сигналізації є реєстрація змін електричного опору елементів, що проводять струм при дотику до них. Помилкові вмикання сигналізації можуть бути викликані тваринами, рослинністю або забрудненням ізоляторів.

Останнім часом зʼявилися системи, засновані на інших принципах.

Системи обʼємного *контролю помешкань і територій*. Вони засновані на тому, що фіксується обʼємне поле, утворене датчиком-генератором (надвисокі частоти, інфрачервоні промені, ультразвук і ін). При появі стороннього обʼєкта конфігурація поля змінюється, що і фіксується приймачем.

Системи, що *реагують на зміну яких-небудь фізичних параметрів* оптичних кабелів при торканні й ін.

У механічних системах захисту території (огорожа, будинки, стіни, вікна і т.д.) використовуються різноманітні датчики: вібраційні, акустичні, електричні перемикачі (з контактами), електричні дротові елементи (спрацьовування відбувається при їх деформації). Значне поширення знайшли телевізійні системи спостереження й оповіщення.

Для запобігання вторгненню на територію, що охороняється, використовується система, у якій знаходять застосування освітлювальні або звукові сигнальні установки. В обох випадках порушник, що намагається проникнути на територію, яка охороняється, інформується про те, що він виявлений охороною, що справляє цілеспрямований психологічний вплив. Крім того, використання освітлювальних установок забезпечує сприятливі умови для дій охорони.

Складні комплекси захисту територій, що охороняються, які складаються, як правило, із декількох систем, можуть ефективно функціонувати за умови, що робота всіх технічних установок постійно контролюється й управляється центральним пристроєм.

Врахувавши підвищене психологічне навантаження чергових центрального поста, необхідність оперативної виробітки і реалізації оптимальних рішень у випадку тривоги, до центральних пристроїв комплексів захисту пред’являються особливі вимоги. Вони мають забезпечувати автоматичне виконання всіх необхідних процедур. У пристрої пам’яті повинен бути записаний перелік заходів, що здійснюються при вмиканні на центральному посту сигналізації тривоги. Доцільно, щоб цей перелік автоматично виводився на екран монітора. Важливу роль відіграє і рівень ергономіки апаратури, якою споряджаються робочі місця чергових охоронців.

Відповідно до сучасних вимог, центральний пристрій повинен забезпечувати автоматичну реєстрацію і відображення всіх повідомлень, що надходять на центральний пост, і сигналів тривоги. Відображення повідомлень здійснюється за допомогою монітора, на екран якого виводиться схематичний план території, що охороняється, з оцінками датчиків системи, які спрацювали, та оповіщення.

Відоме також застосування **шумоподібних (широкосмугових) сигналів (ШСС**) для пристроїв охоронної сигналізації по радіоканалу.

При розробці вітчизняних радіосистем аудіоконтролю необхідне виконання таких основних вимог, як підвищена скритість для пошукового приймача, висока перешкодозахищеність каналу передачі, широкий частотний діапазон, якісна передача аудіоінформації. Тільки застосування ШСС дозволяє задовольнити цим великим вимогам. Для зниження можливості виявлення радіолінії пошуковим приймачем у схему вводяться елементи дистанційного керування (ДК). Введення додаткового радіоканалу керування дозволяє з урахуванням специфіки застосування істотно знизити енергозатрати при роботі системи аудіоконтролю в пасивному режимі.

При цьому, розглядаються два види сигналів, що відрізняються засобом введення інформаційної складової: ШСС1 − фазова маніпуляція несучої частоти двома квазіортогональними псевдовипадковими послідовностями (ПВП), ШСС2 − частотна модуляція з інформаційним сигналом несучої частоти з фазовою маніпуляцією, що кодовиробляє ПВП. Практична реалізація пристрою аудіоконтролю орієнтована на використання одного з видів сигналів.

Практична реалізація приймачів шумоподібних сигналів можлива тільки на основі спеціального кореляційного опрацювання, розробленого і застосованого в космічних засобах передачі інформації, радіонавігації, радіолокації і сотових мережах звʼязку. З іншого боку, якісна передача інформації в системах аудіоконтролю потребує, щоб швидкість передачі була не менше 100 Кбіт/с. Сучасна елементна база дозволяє забезпечити побудову тракту приймального пристрою зі смугою проміжної частоти = 10-20 МГц. У такому випадку потенційний виграш з опрацювання ШСС, що подає собою відношення вихідного сигналу сигнал/перешкода до вхідного, − складе 20 дБ. Забезпечення такого виграшу багато в чому визначається тим, наскільки вдало буде обраний тип ШСС. При цьому припускається як вибір ПВП, так і засіб введення інформаційного сигналу. Мінімально можливе значення відношення сигнал/перешкода на вході обмежується чутливістю приймальної частини системи. Використовуване кореляційне опрацювання ШСС є оптимальне при наявності перешкоди типу білого шуму. На практиці виникають додаткові втрати за рахунок впливу інших перешкод.

Інформаційні джерела.

1. **Комплексні системи захисту інформації** [Текст]: конспект лекцій для студентів напрямку підготовки 125 «Кібербезпека» денної форми навчання / уклад. В.М. Мельник. – Луцьк: Луцький НТУ, 2016. – 68 с.