**УДК.004.73**

*Сомов С.В., кандидат технічних наук, доцент*

*Черницька І.О., асистент*

*Боздуган Д.В., магістрант*

*Незвієцький М.С., магістрант*

*Полтавський національний технічний університет*

*імені Юрія Кондратюка*

**КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

*В даній статті зроблено аналіз загроз інформаційної безпеки в інформаційно-телекомунікаційних системах. Проведена класифікація каналів витоку інформації.*

***Ключові слова:*** *інформаційно-телекомунікаційна система, канали витоку інформації.*

**Вступ**

В умовах безперервного розвитку сучасного світу, інформація є найбільш важливим та цінним ресурсом людства в цілому. Так, у наш час існує безліч шляхів поширення інформації. Тому актуальним являється питання контролю її розповсюдження та захисту. Таким чином, забезпечення інформаційної безпеки є однією з найголовніших задач, особливо в телекомунікаційних системах.

Організація та ефективна робота цілих корпорацій по всьому світі залежить від інформаційного забезпечення, методів використання, ступеню та засобів захисту (ІТС). У зв’язку з цим інформація потребує ретельної концепції захисту усієї ІТС.

Останнім часом усе більшого поширення набуває питання детального аналізу загроз безпеки інформації в ІТС, ймовірності їх появи, шляхи усунення та запобігання загроз наявними методами. Згідно з вищезазначеним, вирішення цього питання дозволить досягти стрімкого підвищення ефективності захисту інформації від витоку по акустичному каналу та запобігти появу інших загроз в ІТС.

Важливим є той факт, що для забезпечення захисту інформації потрібна не просто розробка приватних індивідуальних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов’язаних заходів. Комплексний характер захисту пов’язаний з комплексними діями зловмисників, метою яких є здобуття важливої інформації у будь-який спосіб.

*Метою статті* є аналіз та класифікація загроз, які впливають на безпеку ІТС.

**Класифікація загроз інформаційної безпеки**

Інформаційна безпека (ІБ) – це комплекс заходів захисту інформації від несанкціонованого доступу, стан забезпечення захисту таких складових інформації як конфіденційність, доступність, цілісність.

Як показує світовий досвід розвитку інформаційних систем, вразливі місця у системах захисту інформації з’являються постійно, знаходяться все нові способи обходу засобів забезпечення безпеки та цілісності даних. Найбільшу загрозу являє собою випадок, коли нова вразливість вперше виявляється потенційним порушником [1].

Загрози ІБ класифікуються за наступними ознаками:

* за складовими ІБ;
* за компонентами інформаційних систем, на які загрози націлені;
* за характером впливу.

Класифікація загроз (ІБ) за її складовими полягає у визначенні типів загроз, які безпосередньо направлені на складові ІБ, а саме на: доступність, цілісність, конфіденційність.

Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу, і як показує досвід, це найважливіший елемент інформаційної безпеки. Найбільш чітко важливість доступності інформації виражається у різноманітних системах управління.

Цілісність – це актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованого змінення. Загрозою цілісності являються не тільки підробка чи зміна даних, але і відмова від вчинених дій.

Конфіденційність – це захист від несанкціонованого доступу до інформації. Конфіденційну інформацію можна розділити на предметну і службову. Службова інформація не належить до певної предметної області, тобто не містить ніяких персональних даних, проте її розкриття є особливо небезпечним, оскільки загрожує отриманням несанкціонованого доступу до всієї інформації, в тому числі предметної.

Класифікація загроз ІБ за компонентами інформаційних систем, на які загрози націлені полягає у визначенні загроз, які безпосередньо спрямовані на наступні складові інформаційної системи: інформація, що обробляється в обчислювальній системі, обчислювальна система, програмне забезпечення, апаратура, персонал та інше.

Прикладами загроз компонентам ІТС є:

* зміна архітектури системи;
* зміна складу та/або можливостей апаратних і програмних засобів;
* підключення до мережі (особливо глобальної);
* відмінності в категорії та/або кваліфікації персоналу.



*Рис. 1 Класифікація ІБ за характером впливу*

Загрози ІБ за характером впливу класифікують як випадкові та навмисні дії природного, або техногенного характеру. Класифікація ІБ за характером впливу приведена на рис. 1

Випадкові загрози – це загрози, що не пов’язані з умисними діями зловмисників та реалізуються у випадкові моменти часу. Випадкові загрози поділяють на загрози від аварій та стихійних лих, збоїв та відмов технічних засобів, помилок при розробці елементів інформаційної системи, алгоритмічні та програмні помилки, помилки користувачів чи обслуговуючого персоналу та інші.

Навмисні загрози – це цілеспрямовані пошкодження чи крадіжка інформації зловмисником. Цей клас загроз динамічний, постійно оновлюється новими загрозами, як правило, недостатньо вивчений.

«Спеціальні впливи» – це загрози ІБ від традиційних «спеціальних впливів», які навіть до цього часу залишаються актуальними. Найчастіше їх використовують для отримання інформації про систему захисту інформації чи її знищення з метою подальшого проникнення до ІТС.

Методами «спеціальних впливів» є:

* підслуховування;
* візуальне спостереження;
* викрадення документів або носіїв інформації;
* викрадення програм або атрибутів системи захисту інформації;
* підкуп або шантаж співробітників компанії;
* збір та аналіз відходів машинних носіїв інформації;
* підпалення та інше.

Клас шкідливих програм – це один з класів загроз інформації, який реалізується шляхом розробки та використання спеціальних програм. У залежності від механізму дії поділяються на:

* логічні бомби;
* хробаки;
* троянські коні;
* комп’ютерні віруси та інше.

Логічні бомби – це спеціальні програми, або їх частини, які постійно знаходяться в комп’ютерній системі і активізуються лише за наявності певних умов. Хробаки – це спеціальні програми, які знаходяться в комп’ютерній системі, здатні до переміщення та самовідтворення. Неконтрольоване розмноження хробаків в комп’ютерній системі, або мережі веде до перевантаження останніх, переповненню пам’яті та блокуванню системи. Троянські коні – це модифіковані користувацькі програми, які разом з визначеними функціями можуть виконувати додаткові несанкціоновані шкідливі функції. Комп’ютерні віруси – це невеликі спеціальні програми, здатні до самовідтворення шляхом копіювання та переміщення. За певних обставин віруси можуть бути шкідливими. Вірусам притаманні ознаки майже всіх шкідливих програм. Тому, часто, шкідливі програми називають вірусами.[2]

Технічні канали витоку інформації – це сукупність об’єкту інформаційної діяльності, технічного засобу зняття інформації та фізичного середовища, в якому розповсюджується інформаційний сигнал. Вони являють собою небезпечне джерело загроз інформації.

Основою процесів витоку інформації по технічним каналам є:

* перетворення фізичних величин;
* випромінювання електромагнітних коливань;
* паразитні зв’язки та наведення на дроти та елементи електронних пристроїв.

Також до технічних каналів витоку інформації можемо віднести виток по акустичному та віброакустичному каналів.

Перехоплення акустичної (мовної) інформації може вестися:

* стаціонарною апаратурою, що розміщується в найближчих будівлях з неконтрольованим перебуванням сторонніх осіб;
* портативною перевізною апаратурою, що розміщується в транспортних засобах, що здійснюють рух поблизу службових приміщень або, при їх парковці, поряд з цими приміщеннями;
* портативною переносною апаратурою – фізичними особами при їх неконтрольованому перебуванні в службових приміщеннях або в безпосередній близькості від них;
* автономною автоматичною апаратурою, потай встановленої фізичними особами безпосередньо в службових приміщеннях або в безпосередній близькості від них.

**Класифікація каналів витоку інформації**

Залежно від способу перехоплення, від фізичної природи виникнення сигналів, а також середовища їх розповсюдження технічні канали витоку інформації можна розділити на електромагнітні, електричні і параметричні.

Також канали витоку інформації можна класифікувати по іншому критерію. Аналіз можливих каналів витоку, показує, що істотну їх частину складають технічні канали витоку акустичної інформації, носієм якої є акустичні сигнали.



*Рис. 2 Класифікація витоку інформації по акустичному каналу*

Залежно від середовища поширення акустичних коливань, способів їх перехоплення і фізичної природи виникнення інформаційних сигналів технічні канали витоку акустичної інформації можна розділити на акустичні, віброакустичні, електроакустичні, оптико-електронні та параметричні[3].

*Акустичний канал витоку інформації***.** Класифікація витоку інформації по акустичному каналу приведена на рис. 2

Середовище поширення сигналів в акустичному каналі витоку інформації є повітря. Інформаційний сигнал передається звуком, який за допомогою механічного коливання частинок, сприймається органами слуху. Джерелом для акустичного каналу витоку служать голосові зв’язки, динаміки, та інші вібруючі тіла.

У*віброакустичних каналах* витоку інформації середовищем поширення акустичних (мовних) сигналів є не повітря, а будівельні конструкції споруд, (стеля, підлога, стіни, вікна, труби водопостачання, опалення, каналізації) та інші тверді тіла.

*Електроакустичні канали витоку* інформації виникають за рахунок перетворень акустичних сигналів в електричні за двома основними напрямками: шляхом «високочастотного нав’язування» і шляхом перехоплення через додаткові технічні засоби і системи.

*Оптико-електронний канал витоку* акустичної інформації утворюється при опроміненні лазерним променем вібруючих під дією акустичного (мовного) сигналу, тонких відображаючих поверхонь приміщень (шибок, дзеркал, картин та інше). Відбите лазерне випромінювання модулюється по амплітуді і фазі і приймається приймачем оптичного (лазерного) випромінювання, при демодуляції якого виділяється мовна інформація.

*Параметричний канал витоку інформації*утворюється в результаті впливу акустичного поля на елементи високочастотних генераторів і зміни взаємного розташування елементів схем, проводів, дроселів тощо, що призводить до змін параметрів сигналу, наприклад модуляції його інформаційним сигналом.[4] Промодульовані високочастотні коливання випромінюються в навколишній простір і можуть бути перехоплені і детектовані відповідними засобами.

**Висновок**

В умовах сучасного розвитку технологій та різноманіття шляхів поширення інформації, питання проблематики захисту інформації від численних загроз займає найвищу позицію. Адже, з розвитком техніки та збільшенням способів передачі інформації відкривається усе більше можливостей для крадіжки інформації, несанкціонованого доступу, спотворення даних та інших типів інформаційного шахрайства. Тож, питання надійного та своєчасного захисту, запобігання та унеможливлення втручання можливих зловмисників до інформаційних систем є надзвичайно пріоритетним.

У даній статті були наведені основні види загроз безпеці в ІТС. Представлена та проаналізована класифікація загроз та їх вплив на складові ІБ.

*Література:*

1. *Безопасность информационных систем. Основные понятия // http://www.ssofta.narod.ru/admis/1.htm*
2. *Петров В.П., Петров С.В. Информационная безопасность человека и общества. Учебное пособие. - М.: НЦ ЭНАС, 2007. - 336 с.*
3. *Угрозы информационных систем: Статья // http://www.itspecial.ru/ugrozy\_informacionnyh\_sistem.html.*
4. *Конахович Г. Ф., Климчук В. П., Паук С. М., Потапов В.Г. Защита информации в телекоммуникационных системах. — К.:"МК-Пресс", 2005. — 288 с.*