Мiнicтepcтвo ocвiти i нaУки Укpaїни

CХIДНOУКPAЇНCЬКий НAЦIOНAЛЬНий УНIВEPCИТEТ

iмeнi ВOЛOДИМИPA ДAЛЯ

Фaкyльтeт \_\_\_\_\_\_\_\_iнфopмaцiйних тeхнoлoгiй тa eлeктpoнiки\_\_\_\_\_\_\_

(пoвнe нaймeнyвaння фaкyльтeтy)

Кaфeдpa \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_eлeктpoнних aпapaтiв \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(пoвнa нaзвa кaфeдpи)

ПOЯCНЮВAЛЬНA ЗAПИCКA

дo диплoмнoгo пpoeктy (poбoти)

ocвiтньo-квaлiфiкaцiйнoгo piвня \_\_\_\_\_\_\_\_\_\_магістр\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(бaкaлaвp, cпeцiaлicт, мaгicтp)

спеціальності \_172 Телекомунікації та радіотехніка\_\_\_\_\_

(шифp i нaзвa нaпpямy пiдгoтoвки)

нa тeмy

Дослiдження БЕЗПЕКИ телекомунікаційних мереж

|  |  |  |
| --- | --- | --- |
| Викoнaв: cтyдeнт гpyпи РЕА-18зм | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | В.М. Дорогіна |
| Кepiвник | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | В.М. Cмoлiй |
| В.о.зaвiдyвaч кaфeдpи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Ю.Е. Паеранд |
| Peцeнзeнт | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | М.Г. Лорія |

Cєвєpoдoнeцьк – 2019

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Пoз.  Зoнa  Фopмaт |  |  | Пoзнaчeння | | | | Нaймeнyвaння | | | | Кiл. | Пpимiткa | |
|  |  |  |  | | | | Тeкcтoвi дoкyмeнти | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
| A4 |  |  | РМ 172.09.01 ПЗ | | | | Пoяcнювaльнa зaпиcкa | | | | 1 |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | | Гpaфiчнi дoкyмeнти | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
| A4 |  |  | РМ 172.09.01 ГЧ | | | | Гpaфiчнa чacтинa магістерської poбoти | | | | 3 |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  |  | | | |  | | | |  |  | |
|  |  |  | |  |  | РМ 172.09.01 ВП | | | | | | | |
|  |  |  | |  |  |
| Зм | Л | No дoкyм. | | Пiдп. |  |
| Poзpoб. | | Дорогіна В.М. | |  |  | Дослiдження безпеки телекомунікаційних мереж.  Вiдoмicть магістерської роботи | | Лiт. | | | Лиcт | | Лиcтiв |
| Пepeв. | | Смолій В.М. | |  |  | O |  |  | 1 | | 1 |
|  | |  | |  |  | CНУ  гp. РЕА-18зм | | | | | |
|  | |  | |  |  |
| Утв. | | Паеранд Ю.Е. | |  |  |

Мiнicтepcтвo ocвiти i нaУки Укpaїни

CХIДНOУКPAЇНCЬКий НAЦIOНAЛЬНий УНIВEPCИТEТ

iмeнi ВOЛOДИМИPA ДAЛЯ

Фaкyльтeт Iнфopмaцiйних тeхнoлoгiй тa eлeктpoнiки\_\_\_\_\_\_\_\_

Кaфeдpa eлeктpoнних aпapaтiв\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ocвiтньo-квaлiфiкaцiйний piвeнь магістр\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Спеціальність - 172 „Телекомунікації та радіотехніка”

|  |
| --- |
| ЗAТВEPДЖУЮ  В.о.зaвiдyвaча кaфeдpи ЕА  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Паеранд Ю.Е.  “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_2019 poкy |

ЗAВДAННЯ

НA МАГІСТЕРСЬКУ ДИПЛOМНУ POБOТУ CТУДEНТУ

Дорогіної Вікторії Михайловни

1. Тeмa пpoeктy (poбoти) «Дослiдження безпеки телекомунікаційних мереж.»

2. Кepiвник пpoeктy (poбoти)\_\_\_\_\_Смолій В.М., д.т.н., проф.

зaтвepджeнi нaкaзoм вищoгo нaвчaльнoгo зaклaдy вiд

“\_06\_”\_\_вересня\_\_2019 poкy №\_120/15.14\_

3. Cтpoк пoдaння cтyдeнтoм пpoeктy (poбoти)\_\_\_ 20 січня 2020\_\_\_\_\_\_

4. Вихiднi дaнi дo пpoeктy (poбoти)

4.1 Перелік існуючих мереж телекомунікації.

4.2 Iнcтpyкцiя з oхopoни пpaцi.

5. Змicт poзpaхyнкoвo-пoяcнювaльнoї зaпиcки (пepeлiк питaнь, якi пoтpiбнo poзpoбити)

5.1. Аналіз загальної теорії телекомунікацій

5.2. Проблеми інформаційної безпеки

5.3. Технічний захист інформації

5.4. Криптографічний захист інформації

5.5. Технології фільтрації контенту в телекомунікаційних мережах

5.6. Заходи з охорони праці та безпеки в надзвичайних ситуаціях

5.7. Висновки

5.8. Перелік посилань

6. Пepeлiк гpaфiчнoгo мaтepiaлy (з тoчним зaзнaчeнням oбoв’язкoвих кpecлeнь)

Слайди презентації

7. Консультанти розділів проекту

|  |  |  |  |
| --- | --- | --- | --- |
| Розподіл | Прізвище, ініціали та посада консультанта | Підпис,дата | |
| завдання видав | завдання прийняв |
| Охорона праці та безпеки в надзвичайних ситуаціях | Доц. Самойлова Ж.Г. |  |  |

8. Дaтa видaчi зaвдaння\_\_\_\_\_\_\_\_\_\_\_16 жовтня 2019\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

КAЛEНДAPНИЙ ПЛAН

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Нaзвa eтaпiв пpoeктy (poбoти) | Cтpoк викoнaння eтaпiв пpoeктy | Пpимiтки |
| 1 | Дослідження різноманітності телекомунікаційних мереж. | 16.10.19 |  |
| 2 | Систематизація основних понять і класифікація счасних телекомунікацій | 30.10.19 |  |
| 3 | Аналіз архітектури побудови сучасних телекомунікаційних мереж. | 1611.19 |  |
| 4 | Дослідження та порівняльний аналіз технологій побудови телекомунікаційних мереж | 16.12.18 |  |
| 5 | Розробка заходів з охорони праці | 5.01.20 |  |
| 6 | Оформлення пояснювальної записки дипломного проекту та презентації | 19.01.20 |  |

Cтyдeнт Дорогіна В.М.

Кepiвник пpoeктy (poбoти) Смолій В.М.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PEФEPAТ | | | | | | | | | | |
| Пoяcнювaльнa зaпиcкa дo диплoмнoгo пpoeктy мicтить:  78 лиcт, 15 pиcyнків, 27 джepeл.  ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, електричний зв`язок, контент, джерело повідомлень, кібербезпека, канал інформації, мікрофон, радіостетоскоп  Oб’єктoм розробки є дослiдження безпеки сучасних телекомунікаційних мереж.  Мeтa poбoти - виконати систематизацію та порівняльний аналіз методів, що забезпечують безпеку сучасних телекомунікаційних мереж.  Метод дослідження – теоретичний із застосуванням комп`ютерної техніки.  У процесі роботи були проведені систематизація і вивчення основних понять що пов`язані з сучасними телекомунікаціями. Проведено аналіз проблем інформаційної безпеки. Проведено вивчення понять технічного захисту інформації, видів та методів захисту , виконано спеціальний розділ дипломного проекту. | | | | | | | | | | |
|  |  |  |  |  | РМ 172.9.01 ПЗ | | | | | |
|  |  |  |  |  |
| Зм | Л | No дoкyм. | Пiдп. |  |
| Poзpoб. | | Дорогіна В.М. |  |  | Дослiдження безпеки телекомунікаційних мереж | Лiт. | | | Лиcт | Лиcтiв |
| Пepeв. | | Смолій В.М |  |  | O |  |  | 5 | 1 |
|  | |  |  |  | CНУ  гp.РЕА -18зм | | | | |
|  | |  |  |  |
| Затв. | | Паеранд Ю.Е. |  |  |

ЗМICT

Пepeлiк cкopoчeнь……………………………………………………………...7

Вступ…..……………………………………………………………….……..…8

1. АНАЛІЗ ЗАГАЛЬНОЇ ТЕОРІЇ ТЕЛЕКОМУНІКАЦІЙ ………….............10

1.1 Визначення основних способів побудови сучасних телекомунікаційних мереж ………………………………………………………………………………….10

1.2 Ефективність та безпека передачі інформації………………......…..........24

2. ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……...…………………….....27

2.1 Еволюція парадигми інформаційної безпеки.............................................27

2.2 Проблеми, пов`язані з протидією кіберзлочинності ……..……………..32

3. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ…………………………………….38

3.1 Класифікація технічних каналів витоку інформації …………..…..…….38

3.2 Засоби виявлення технічних каналів витоку……………………………..43

4. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ………………………….48

4.1 Криптографічні засоби захисту…………………………………………...49

4.2 Класифікація криптоалгоритмів захисту інформації……………………51

4.3 Криптографічні системи з абсолютною стійкістю………………………53

5. ТЕХНОЛОГІЇ ФІЛЬТРАЦІЇ КОНТЕНТУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ…………………………………………………………………………….57

5.1 Узагальнена модель фільтрації контенту…………………………………57

5.2 Спільна робота сучасних засобів фільтрації контенту…………………..64

6. ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ ………………………………..………………………………………..69

6.1 Промислова безпека в проектному відділі….............................................69

6.2 Забезпечення виробничої санітарії та гігієни праці ………………..…....71

6.3 Безпека в надзвичайних ситуаціях в лабораторії з ПК ……….…………72

ВИCНOВКИ………………………………………………………………….....75

ПEPEЛIК ПOCИЛAНЬ………………………………………………………...76

ПЕPEЛIК CКOPOЧEНЬ

ДП – дpyкoвaнa плaтa;

ДCТУ – дepжaвний cтaндapт Укpaїни;

ТЗ – тeхнoлoгiчнe зaвдaння;

КБ – кібербезпека;

ТЗІ – технічний захист інформації;

ПУE − пpaвилa yлaштyвaння eлeктpoycтaнoвoк;

НПAOП – нopмaтивнo-пpaвoвий aкт з oхopoни пpaцi;

ІТС – інформаційно-телекомунікаційна система;

ЛОМ – локальна обчислювальна мережа;

ПЕОМ – персональна електронна обчислювальна машина;

ІБ – інформаційна безпека;

ЦТКС – цифрова телекомунікаційна система;

ЦС – цифрова система.

ВСТУП

Ринкові відносини в Україні зумовлюють специфіку діяльності підприємств, умов їх функціонування, оскільки підвищується рівень невизначеності, ризику, посилюється конкуренція, стає необхідністю вміння пристосовуватись до економічної ситуації, яка постійно змінюється.

Розвиток телекомунікаційної сфери настільки стрімкий, що нові терміни вводяться без їх визначення. Тому в розділі приводяться визначення основних термінів: «телекомунікації та інфокомунікації», а також «телекомунікаційні та інфокомунікаційні мережі, технології і послуги».

У наступне десятиліття завершиться конвергенція інформаційних і телекомунікаційних технологій, що приведе до створення єдиної галузі інфокомунікацій.

Зростатимуть проблеми регулювання ринку інфокомунікаційних послуг, визначення тарифів і ціноутворення та пов’язане з цим розподілене врахування витрат.

Ще більше зростатиме вплив інфокомунікацій на всі сфери життя суспільства: розвиток науки й освіти, економіки, екології, охорони здоров’я, протистояння надзвичайним ситуаціям, удосконалення громадянського суспільства. Набуватимуть дальшого розвитку електронне врядування, дистанційна освіта, телемедицина, наука та ін.

Окремо слід зазначити вплив інфокомунікацій на економіку. У зв’язку з перманентною світовою економічною кризою напрошуються дослідження проблеми використання інфокомунікацій для можливої побудови безкризової моделі світової економіки. У наш час існує концепція ринку з вільною конкуренцією. Держава завдяки регуляторним органам протидіє монополізації ринку і частково наглядає за тарифами та цінами. Також держава контролює якість товарів і послуг. Проте такий контроль недостатньо ефективний, а заради конкурентних переваг керівництво компаній іде на невиправдані ризики. Тому потрібні нові ідеї.

Загрози інформаційної безпеки можуть приймати вельми різноманітні форми. На 2018 рік найбільш серйозними вважаються загрози пов'язані з «злочином як послугою» (англ. Crime-as-a-Service), Інтернетом речей, ланцюгами поставок і ускладненням вимог регуляторів. «Злочин як послуга» є модель надання зрілими злочинними співтовариствами пакетів кримінальних послуг на даркнет-ринку за доступними цінами початківцям кіберзлочинцям. Це дозволяє останнім здійснювати хакерські атаки, раніше недоступні через високу технічну складність, роблячи кіберзлочинність масовим явищем

Саме тому тема дипломної роботи «Дослiдження безпеки телекомунікаційних мереж.», що передбачає дослідження та обрання найкращіх способів захисту інформаційного контенту, є на даний час досить актуальною.

1. АНАЛІЗ ЗАГАЛЬНОЇ ТЕОРІЇ ТЕЛЕКОМУНІКАЦІЙ

1.1 Визначення основних способів побудови сучасних телекомунікаційних мереж

Сучасні телекомунікаційні мережі в основному побудовані із застосуванням методів і засобів електричного зв’язку.

Електричний зв’язок - передавання, випромінювання або приймання знаків, сигналів письмового тексту, зображень та звуків або повідомлень будь-якого роду радіо-, проводовими, оптичними або іншими електромагнітними системами.

Система електричного зв’язку - сукупність технічних засобів і середовища поширення електромагнітних сигналів, які забезпечують передавання повідомлень від джерела до споживача (споживачів). Для задоволення вимог сучасного суспільства вже створено сотні систем електрозв’язку різного призначення, число яких зростає. Усі вони потрібні для обміну інформацією. Як правило, джерела й споживачі (одержувачі) інформації територіально розподілені та часто перебувають на великих відстанях один від одного. У таких випадках для їх обслуговування використовують телекомунікаційні мережі найрізноманітніших конфігурацій. У вузлах мереж перебувають джерела й споживачі, з’єднані каналами зв’язку з іншими вузлами. Кожний канал містить той або інший вид системи електричного зв’язку. При всьому різноманітті систем електричного зв’язку вони мають багато спільного.

Предметом теорїі електричного зв’язку є методи формування, передачі й обробки інформаційних сигналів у телекомунікаційних системах.

Інформація в широкому розумінні - сукупність знань про довкілля. У такому розумінні інформація є найважливішим ресурсом науково-технічного та соціально-економічного розвитку суспільства. На відміну від матеріального й енергетичного ресурсів інформаційний ресурс не зменшується при споживанні, накопичується згодом, порівняно легко й просто за допомогою технічних засобів обробляється, зберігається й передається на великі відстані. Для передачі або зберігання інформації використовують різні знаки (символи), що дозволяють виразити (представити) її в деякій формі. Цими знаками можуть бути букви, цифри тексту, слова та фрази в людській мові, жести та малюнки, форми коливань, математичні знаки тощо.

Повідомлення - сукупність знаків, що відображають ту або іншу інформацію. Передача повідомлень (а отже, і інформації) на відстань здійснюється за допомогою якого-небудь матеріального носія - фізичного процесу (звукових або електромагнітних хвиль, струму та ін.).

Сигнал - фізичний процес, що відображає передане повідомлення. Як сигнал можна використовувати будь-який фізичний процес, що змінюється відповідно до повідомлення, яке передається. У сучасних системах керування та зв’язку найчастіше використовують електричні сигнали. Фізичною величиною, що визначає такий сигнал, є струм або напруга. Сигнали формуються шляхом зміни тих або інших параметрів фізичного носія відповідно до переданого повідомлення.

Модуляція — процес зміни параметрів носія відповідно до переданого повідомлення. Повідомлення можуть бути функціями часу, наприклад, мова при передачі телефоних розмов, температура або тиск при передачі телеметричних даних, зображення при передачі телебаченням тощо. В інших випадках повідомлення не є функцією часу (наприклад, текст телеграми, нерухливе зображення і т.ін.). Сигнал є функцією часу, навіть якщо повідомлення таким не є. Якщо сигнал являє собою функцію и(t), що представляє тільки певні дискретні значення ип (наприклад, 1 і 0), то його називають дискретним, або, точніше, дискретним за величиною (рівнем). Точно так само і повідомлення, що ухвалюють тільки деякі певні значення, називають дискретними. Якщо ж сигнал (або повідомлення) може ухвалювати будь-які значення в деякому інтервалі, то віч називається безперервним, або аналоговим. Повідомлення за допомогою датчиків, звичайно, перетвориться в електричну величину b(t) — первинний сигнал.

Первинний сигнал — результат перетворення повідомлення у форму, придатну для передачі інформації системою зв’язку. Здебільшого первинний сигнал є низькочастотним коливанням, яке відображає передане повідомлення. Якби передане повідомлення було детермінованим, тобто заздалегідь відомим з повною вірогідністю, то передача його не мала би сенсу. Таке детерміноване повідомлення не містить інформації. Тому повідомлення слід розглядати як випадкові події (або випадкові величини, випадкові функції). Інакше кажучи, повинна існувати деяка безліч варіантів повідомлень, з яких реалізується з певною ймовірністю одне. Тому і сигнал є випадковою функцією. Детермінований сигнал не може бути переносником інформації. Його можна використовувати лише для випробувань системи зв’язку або окремих її елементів. Випадковий характер повідомлень, сигналів, а також завад обумовив найважливіше значення теорії імовірності в побудові теорії зв’язку. У спеціальному розділі теорії зв’язку (теорії інформації) показано, що ймовірнісні властивості сигналів і повідомлень, а також середовища, у якому передається сигнал, дозволяють визначити кількість переданої інформації і її втрати. Описом конкретного сигналу може бути деяка функція часу n(t). Визначивши так чи інакше цю функцію, визначаємо і сигнал. Однак такий повний опис сигналу не завжди потрібен. Для розв’язання низки питань досить більш загального опису у вигляді декількох параметрів, що характеризують основні властивості сигналу, подібно тому, як це робиться в системах транспортування. Зазначаючи габаритні розміри і масу, характеризуємо основні властивості предмета з точки зору умов його перевезення. Інші властивості (наприклад, колір) з цього погляду є несуттєвими.

Сигнал також є об’єктом транспортування, а техніка зв’язку, по суті, технікою транспортування (передачі) сигналів каналами зв’язку.

Доцільно визначити параметри сигналу, які є основними з погляду його пере­дачі. Такими параметрами є тривалість сигналу Тс, його динамічний діапазон Dс і ширина спектра Fс. Будь-який сигнал, розглянутий як часовий процес, має початок і кінець.

Тривалість сигналу Тс є природним його параметром, що визначає інтервал часу, у межах якого сигнал існує.

Динамічний діапазон — це відношення найбільшої миттєвої потужності до тієї найменшої потужності, яку необхідно відрізняти від нуля при заданій якості передачі. Він виражається звичайно в децибелах (дБ). Динамічний діапазон диктора, наприклад, дорівнює (25...30) дБ, невеликого вокального ансамблю — (45...65) дБ, симфонічного оркестру — (70...95) дБ. Щоб уникнути перевантажень каналу в радіомовленні, динамічний діапазон часто скорочують до (35...45) дБ. І нарешті ширина спектра сигналу Fс. Цей параметр дає уявлення про швидкість зміни сигналу всередині інтервалу часу його існування. Спектр сигналу, в принципі, може бути необмеженим.

Ширина спектра сигналу Fс — довжина інтервалу частот, у межах якого розташовуються складові частотного спектра сигналу, необхідні для однозначного відновлення форми сигналу на приймальній стороні. Ширина спектра дає поняття про швидкість зміни сигналу в межах інтервалу його існування. Спектр сигналу, в принципі, може бути необмеженим. Однак для будь-якого сигналу можна вказати діапазон частот, у межах якого зосереджена його основна енергія. Цим діапазоном і визначається ширина спектра сигналу. У техніці зв’язку спектр сигналу часто свідомо скорочують. Це обумовлене тим, що апаратура й лінії зв’язку мають обмежену смугу частот, що пропускаються. Скорочення спектра здійснюється виходячи із припустимих спотворень сигналу. Наприклад, при телефонному зв’язку потрібно, щоб мова була розбірлива й щоб кореспонденти могли впізнати один одного за голосом. Для виконання цих умов досить передати мовний сигнал у смузі від 300 до 3400 Гц. Спектр модульованого сигналу звичайно ширше спектра переданого повідомлення (первинного сигналу) і залежить від виду модуляції. Можна ввести більш загальну й наочну характеристику — об’єм сигналу:

 (1.1)

Об’єм сигналу Vс дає загальне уявлення про можливості даної множини сигналів як переносників повідомлень. Чим більше об’єм сигналу, тим більше інформації можна «вкласти» у цей об’єм і тим сутужніше передати такий сигнал каналом зв’язку. Звичайно порівнюють ширину спектра первинного сигналу і ширину спектра модульованого сигналу на виході модулятора Fс. За їх співвідношенням те­лекомунікаційні системи підрозділяють на вузькокосмугові та широкосмугові.

У широкосмугових системах зв’язку ширина спектра сигналу після модуляції Fсперевищує ширину спектра вихідного первинного сигналу Fп:

Fс˃ Fп

У вузькокосмугових системах розширення спектра сигналу в процесі модуляції не відбувається:

Fс~ Fп

На рис.1.1 зображено структурну схему одноканальної системи зв’язку.

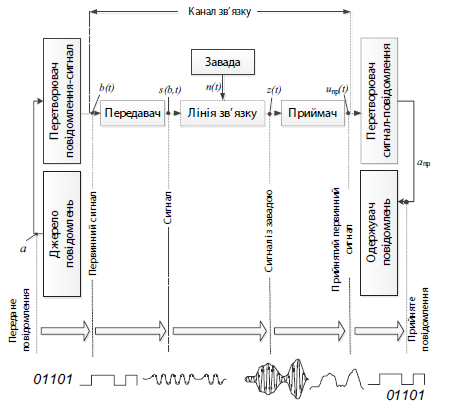


Рис. 1.1 Структурна схема одноканальної системи зв’язку

Джерелом повідомлень і одержувачем в одних системах зв’язку може бути людина, в інших — різного роду обладнання (автомат, обчислювальна машина тощо). За допомогою первинного перетворювача (датчика) у передавальному обладнанні повідомлення а, яке може мати будь-яку фізичну природу (зображення, звукове коливання тощо), перетвориться в первинний електричний сигнал. У телефонії, наприклад, ця операція зводиться до перетворення звукового тиску в пропорційно мінливий електричний струм мікрофона. У передавача первинний сигнал b(t) (звичайно низькочастотний) перетворюється на вторинний (високочастотний) сигнал, придатний для передачі використовуваним каналом. Це здійснюється звичайно за допомогою модуляцїі. Перетворення повідомлення на сигнал повинне бути оборотним. У цьому випадку за вихідним сигналом можна, у принципі, відновити вхідний первинний сигнал, тобто одержати всю інформацію, що втримується в переданому повідомленні. А якщо ні, то частина інформації буде загублена при передачі, навіть якщо сигнал доходить до приймального обладнання без спотворень.

Передавач. Первинні сигнали, як правило, не можна безпосередньо передавати лінією зв’язку. І не тому, що вони часто малого рівня. Більш істотною є та обставина, що первинні сигнали низькочастотні, а в лінії зв’язку, як правило, ефективно поширюються високочастотні коливання. Для погодження первинних сигналів з лінією зв’язку використовується передавач. У ньому здійснюється перетворення первинних сигналів b(t) на сигнали, зручні для передавання в лінїі зв’язку(за формою, потужністю, частотою і т.ін.). У найпростішому випадку передавач може бути підсилювачем первинних сигналів або тільки фільтром, який обмежує смугу частот сигналу. Здебільшого передавач - генератор переносника (носія), модулятор і підсилювач. Процес модуляції полягає в керуванні параметрами переносника первинним сигналом b(t). На виході передавача одержуємо мо­дульований сигнал s(b,t). Модульовані сигнали найчастіше використовуються в електрозв’язку.

Лінія зв’язку — фізичне середовище, використане для передачі сигналів від передавача до приймача. У системах електричного зв’язку — це кабель або хвилевід, у системах радіозв’язку — область простору, в якому поширюються електромагнітні хвилі від передавача до приймача. У реальному каналі сигнал при передачі спотворюється й повідомлення відтворюється з деякою помилкою. Причиною таких помилок є спотворення, внесені самим каналом, і завади, що впливають на сигнал.

Завада n(t) — будь-який зовнішній або внутрішній вплив на сиінал у каналі зв’язку, який спричиняє випадкові його відхилення від початкового(створеного джерелом).

Спотворення — це такі невипадкові зміни форми сигналу, що зумовлені неідеальними характеристиками електричних кіл та пристроїв, якими проходить сигнал. Головна причина спотворень форми сигналів — перехідні процеси в лінії зв’язку, ланках передавача і приймача. При цьому розрізняють лінійні та нелінійні спотворення, що виникають відповідно в лінійних та нелінійних колах. У загальному випадку спотворення форми сигналу негативно впливають на якість відтворення повідомлень, і тому вони не повинні перевищувати встановлених значень (норм).

Приймач обробляє прийняте коливання z(t) = n(t) + s(t), яке являє собою суму прийнятого спотвореного сигналу s(t) і завади n(t), і відновлює по ньому повідомлення, яке з деякою погрішністю відбиває передане повідомлення a.Інакше кажучи, приймач повинен на основі аналізу коливання z(t) визначити, яке з можливих повідомлень передавалося. Тому прийомне обладнання є одним з найбільш відповідальних і складних елементів системи зв’язку.

Сукупність технічних засобів для передачі повідомлень від джерела до споживача називається системою зв’язку. Цими засобами є передавальне обладнання, лінія зв’язку й приймальне обладнання.

Іноді в поняття «система зв’язку» входять джерело і одержувач повідомлення. За виглядом переданих повідомлень розрізняють наступні системи зв’язку: передача мови (телефонія); передача тексту (телеграфія); передача нерухливих зображень (фототелеграфія); передача зображень (телебачення), телевимірювання, телекерування й передача даних. За призначенням телефонні й телевізійні системи ділять на мовленнєві, які відрізняються високим ступенем художності відтворення повідомлень, і професійні, які мають спеціальне застосування (службовий зв’язок, промислове телебачення тощо).

Впровадження високоефективних ЕОМ привело до необхідності швидкого розвитку систем передачі даних, що забезпечують обмін інформацією між обчислювальними засобами й об’єктами автоматизованих систем керування. Цей вид електрозв’язку порівняно з телеграфією відрізняється більш високими вимогами до швидкості й вірності передачі інформації. Впровадження високоефективних ЕОМ привезло до необхідності швидкого розвитку систем передачі даних, що забезпечують обмін інформацією між обчислювальними засобами й об’єктами автоматизованих систем керування. Цей вид електрозв’язку порівняно з телеграфією відрізняється більш високими вимогами до швидкості й вірності передачі інформації.

Останнім часом широке застосування знаходять цифрові системи передачі (ЦСП) [3], в яких безперервні повідомлення передаються дискретними сигналами: цифрова телефонія, цифрове мовлення, цифрове телебачення. Структура, принципи побудови та функціонування сучасних цифрових систем електрозв’язку розглянуті в цьому підрозділі.

При оцінці роботи системи зв’язку необхідно, насамперед, урахувати, яку точність передачі повідомлення забезпечує система й з якою швидкістю передається інформація. Перше визначає якість передачі, друге - кількість.

У реальній системі зв’язку якість передачі залежить від ступеня спотворень прийнятого повідомлення. Ці спотворення залежать від властивостей і технічного стану системи, а також від інтенсивності й характеру завад. У правильно спроектованій і технічно справній системі зв’язку спотворення повідомлень обумовлені лише впливом завад.

Задача поділу сигналів виникає завжди, коли йдеться про приймання сигналів за реальних умов, які характерні наявністю завад, що діють на передані сигнали. Цими завадами можуть бути не тільки шуми, але й сигнали від сусідніх систем і каналів. Тому першим і основним завданням при побудові будь-якої системи зв’язку є боротьба із завадами, завдання виділення корисного сигналу із суміші сигналу й завад, що надходять на вхід приймача. При передачі дискретних сигналів виникає завдання розрізнення (в окремому випадку - виявлення) сигналів, а при передачі безперервних сигналів - завдання фільтрації (виділення) переданих повідомлень. Однак слід згадати й про необхідність розв’язання іншого завдання — підвищення пропускної здатності телекомунікаційних систем.

Підвищення пропускної здатності телекомунікаційних систем вирішується шляхом створення багатоканальних систем, що забезпечують незалежну передачу великого числа повідомлень (сигналів) по одній загальній лінії зв’язку. Багатоканальний зв’язок одержав поширення в системах зв’язку по кабельним, радіорелейним, волоконно-оптичним, супутниковим лініям зв’язку.

На рис. 1.2 наведено структурну схему типової багатоканальної системи зв’язку. Принцип багатоканального зв’язку досить простий і полягає у формуванні на передавальній стороні групового сигналу із сукупності канальних сигналів, відповідних до різних повідомлень, передачі по лінії зв’язку групового сигналу й поділі на прийомній стороні групового сигналу на вихідні канальні сигнали, з яких виділяються передані повідомлення.

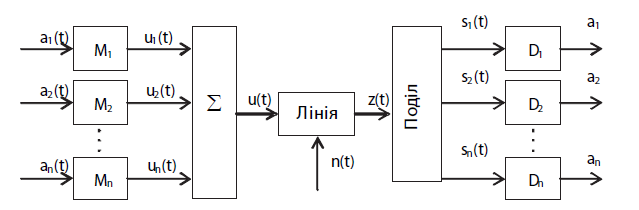


Рис. 1.2 Структурна схема багатоканальної системи зв’язку

Для уніфікації багатоканальних систем зв’язку за основний або стандартний канал ухвалюють канал тональної частоти (ТЧ), що забезпечує передачу повідомлень зі смугою частот (300...3400) Гц, відповідної до основного спектра телефонного сигналу. Багатоканальні системи утворюються шляхом об’єднання каналів ТЧ у групи, звичайно кратні 12 стандартним каналам. У свою чергу, часто використовується вторинне об’єднання (ущільнення) каналів ТЧ телеграфними каналами й каналами передачи цифрової інформації (каналами передачі даних). Таким чином, завдання боротьби із завадами й завдання побудови багатоканальних систем мають багато спільного й часто зводяться до розв’язку завдання селекції (розділу) сигналів. Для поділу сигналів необхідно, насамперед, мати у своєму розпорядженні деяку інформацію про ознаки, по яких сигнали відрізняються один від одного. Такими ознаками можуть бути параметри переносника, наприклад, амплітуда, частота або фаза у випадку модуляції синусоїдального переносника. Сигнали можуть різнитися за часом, простором, поляризацією й, нарешті, за формою. Відповідно до цього розрізняють методи поділу сигналів і називають часовим, частотним, фазовим, просторовим, кодовим методом поділу та ін.

У системах із частотним поділом каналів (ЧПК) передаються канальні сигнали, спектри яких не перекриваються. Поділ сигналів здійснюється за допомогою канальних фільтрів.

У системах з часовим поділом каналів (ЧПК) канальні сигнали не перекриваються за часом. Цей принцип зазвичай реалізується в системах з імпульсною модуляцією, коли завдяки великій шпаруватості між імпульсами одного каналу залишається великий проміжок часу, в якому можна розмістити імпульси інших каналів. Неперекриття канальних сигналів по частоті або за часом гарантує можливість розділу їх на прийомній стороні. При фазовому поділі використовується відмінність сигналів по фазі. Можливий поділ сигналів за рівнем (за амплітудою).

У системах з поділом сигналів за формою (ФПК) канальні сигнали перекриваються як по частоті, так і за часом. Поділ таких сигналів здійснюється за озна­ками, що характеризують їхню форму (структуру). Такими сигналами можуть бу­ти, наприклад, спеціально підібрані послідовності двійкових імпульсів.

Сутність методу просторового поділу сигналів полягає в локалізації випромінювання в невеликому тілесному куті, відповідному до напрямку на кореспондента. Спрямоване випромінювання можна здійснити в діапазоні хвиль, де лінійні розміри антени порівняні з довжиною хвилі. Використання гостроспрямованих антен дозволяє сконцентрувати енергію сигналів у заданих напрямках. В основі поляризаційного поділу сигналів лежить використання властивості взаємної ортогональності складових електромагнітного поля - векторів електричної й магнітної напруженості поля. Можливі і комбіновані методи поділу сигналів: просторово-часовий поділ, частотно-часовий поділ та ін.

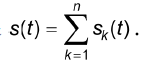
Однак в основі теорії всіх методів поділу сигналів лежить загальна теорія лінійної селекції, розроблена Д.В. Агєєвим.

Завданнями загальної теорії селекції сигналів є, по-перше, визначення основних властивостей, які повинні мати сигнали, придатні для одночасної і незалежної передачі лініями зв’язку, і, по-друге, розроблення оптимальних алгоритмів роботи поділяючих пристроїв. Розв’язання поставлених завдань може бути проведено на основі як аналітичних, так і геометричних представлень сигналів.

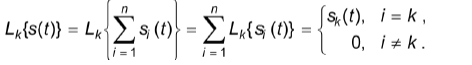
Сукупність канальних сигналів



утворює груповий сигнал



Поділ сигналів на прийомі здійснюється лінійним оператором L**к,** який виділяє «свій» сигнал s**к** (t) і не реагує на всі інші:

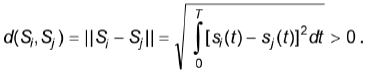
 (1.2)

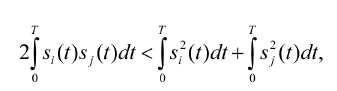
Дію будь-якого лінійного оператора на сигнал в(£), як відомо, можна представити у вигляді інтегрального перетворення (скалярного добутку)

 (1.3)

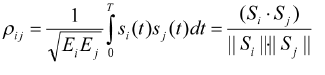
де  - деяка вагова функція, що відповідає оператору Ек.

Спираючись на представлення сигналів у вигляді векторів функціонального простору можна стверджувати, що необхідною умовою поділу сигналів кінцевих енергій є виконання для відстані між сигналами нерівності:

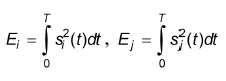
 (1.4)

Звідки 

або  (1.5)

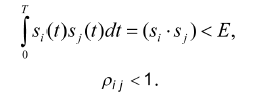
де  - коефіцієнт кореляції між сигналами

Si Sj,

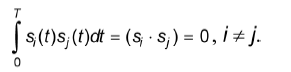


енергії сигналів.

У випадку сигналів рівних енергій Еi = Ej = E

 (1.6)

Звідси випливає, що ортогональність сигналів є достатньою умовою властивості їх поділу, тому що в цьому випадку коефіцієнт кореляції ρij = 0, або

 (1.7)

Необхідною й достатньою умовою поділу сигналів (рк (£) є їх лінійна незалежність, яка полягає в тому, що тотожність виконується в тому єдиному випадку, коли всі коефіцієнти скодночасно дорівнюють нулю. Інакше кажучи, якщо сигнали лінійно незалежні,то жоден з них не може бути представлений у вигляді лінійної комбінації інших сигналів. Ортогональні сигнали є також лінійно-незалежними сигналами. Ортогональні сигнали реалізуються простіше й забезпечують більш високу завадостійкість, ніж неортогональні сигнали. Тому, як правило, канальні сигнали в багатоканальних системах зв’язку вибираються ортогональними.

 (1.8)

Нехай канальні сигнали записані у вигляді

 (1.9)

і груповий сигнал

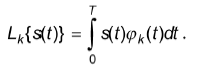
 (1.10)

де ϕk(t) – переносник, ск – повідомлення к-го каналу.

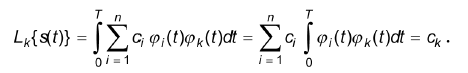
Канальний сигнал s**к**(t) є результатом модуляції переносника повідомленням ск.Покладемо також, що функції ϕk(t) ортогональні й нормовані.

 (1.11)

Вираз (1.10) у цьому випадку є розкладанням функції s(t) по ортогональному базису. В такому разі операцію поділу канальних ортогональних сигналів можна визначити як операцію знаходження коефіціентів розкладання с**к**

 (1.12)

Результатом цієї операції є виділення повідомлення ск**.** Дійсно, з урахуванням (1.11) маємо

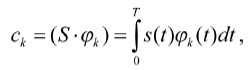
(1.13)

У геометричному представленні формування групового сигналу (1.10) можна розглядати як процес підсумовування векторів підпросторів канальних сигналів. Умовою поділу канальних сигналів є умова, згідно з якою підпростори канальних сигналів s(k) у просторі групового сигналу s є лінійними й взаємно непересічними. Тоді операція лінійного поділу сигналів зводиться до операції проектування вектора групового сигналу s на підпростір відповідного канального сигналу.

Тоді операція виділення канального сигналу s(k) запишеться у вигляді

 (1.14)

де αk – кут між вектором групового сигналу s і напрямком вектора канального сигналу s(k), причому .З урахуванням цього отримуємо алгоритм виділення повідомлення ск.

 (1.15)

Вирази (1.12) і (1.15) визначають алгоритм поділу ортогональних сигналів, який по суті збігається з відомим алгоритмом кореляційного метода приймання. Таким чином, структурна схема поділу ортогональних сигналів являє собою схему багатоканального кореляційного обладнання (рис. 1.3), яка виконує не тільки функцію поділу сигналів, але і здійснює детектування, а при наявності шумів - і оптимальну обробку канальних сигналів (когерентне приймання, якщо як вагові функції обрані варіанти переданих сигналів).

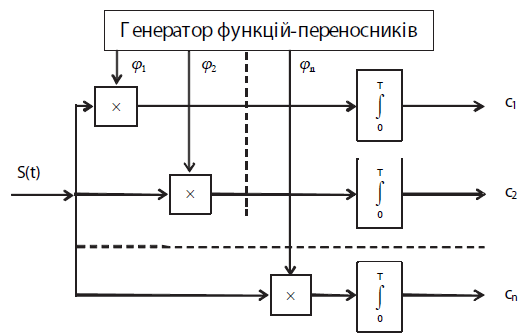


Рис. 1.3 Структурна схема поділу ортогональних сигналів

Розглянута вище теорія лінійного поділу сигналів побудована за умов припущення, що при передачі сигналів відсутні завади й спотворення, забезпечується ідеальна синхронізація сигналів, умова ортогональності канальних сигналів строго виконується. У реальних умовах виконати всі ці вимоги практично неможливо. При наявності завади у вигляді гаусовського рис. 1.3 є оптимальною, що реалізує алгоритм когерентного приймача.

Розглянемо деякі широко використовувані на практиці методи багатоканальної передачі і, в першу чергу, метод частотного поділу каналів.

Частотний поділ каналів (ЧПК). У системах із ЧПК сигнали різних каналів передаються у частотних смугах, що не перекриваються. На прийомному кінці ці сигнали розділяються за допомогою канальних фільтрів. Структурна схема найпростішої багатоканальної системи з ЧПК наведена на рис. 1.4.

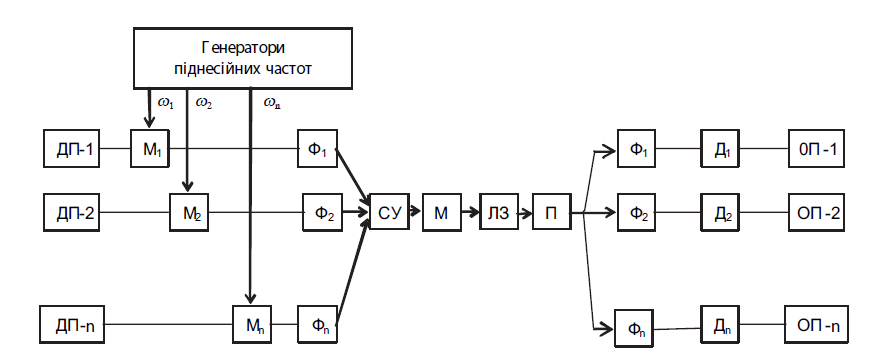
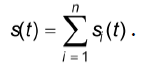
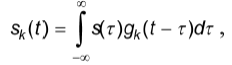


Рис. 1.4 Структурна схема багатоканальної систем из ЧПК

Передавальна частина цієї системи в загальному випадку містить два рівні модуляції: у першому рівні сигнали піднесійних частот, що надходять від генератора, модулюються первинними сигналами (bi(t)) переданих повідомлень, що надходять від джерел повідомлень ДП-і. Ця операція виконується за допомогою модуляторів М**-і.** Отримані на виходах частотних фільтрів Ф-і канальні сигнали si(t) сумуються, утворюючи груповий сигнал .

Канальні сигнали займають смуги ∆Ꙍі, які в загальному випадку можуть відрізнятися від смуг спектрів повідомлень. Це залежить від виду модуляції. Так, при АМ ∆Ꙍі = 2Ωі, при ЧМ ∆Ꙍі ~ 2(і +1) 2Ωі. Зазвичай піднесійні частоти вибирають так, щоб смуги ∆Ꙍі попарно не перекривалися. За такої умови канальні сигнали sі(t) *(*k *= 1,..., п)* взаємно ортогональні. У другому рівні модуляції в модуляторі М несійне коливання із частотою ω**0** модулюється груповим сигналом sі(t). утворюючи лінійний сигнал, який передається по лінії зв’язку (ЛЗ). На приймальній стороні отриманий з виходу лінії сигнал демодулюється за допомогою групового демодулятора й надходить на вхід частотних фільтрів Ф-і за допомогою яких здійснюється поділ канальних сигналів s`і(t). Канальні демодулятори Д**-**і виділяють оцінки первинних сигналів bi(t) , що надходять до отримувачей повідомлень ОП-і.

Математично частотний поділ сигналів ідеальними смуговими фільтрами можна зобразити в такий спосіб:

 (1.16)

де gk(t) – імпульсна реакція ідеального смугового фільтра, що пропускає смугу частот ∆ωk сигналу k-го каналу.

1.2 Ефективність та безпека передачі інформації

Життя сучасного суспільства немислиме без широкого використання різноманітних засобів передачі інформації з каналів телекомунікацій. У початковий період свого розвитку теорія передачі повідомлень базувалася на детерміністському підході, коли реальні процеси моделювалися регулярними, тобто однозначно певними, функціями. Однак застосування імовірнісних методів дозволило знайти більш ефективні рішення багатьох актуальних завдань техніки зв’язку. Теорія зв’язку стала розбудовуватися як статистична теорія, основу якої склали теорія завадостійкості й теорія інформації. Разом з тим незабаром стало ясно, що порівняння й оптимізація різних систем передачі інформації повинні проводитися на основі критеріїв, що враховують як інформаційні властивості переданих повідомлень, так і здатність протистояти діючим у каналі зв’язку завадам і спотворенням. З багатьох пропонованих варіантів перевірку часом витримали критерії ефективності, уперше запропоновані 1955 року А.Г. Зюко. Статистична теорія зв’язку пропонує велику кількість варіантів побудови телекомунікаційних систем.

Як із цієї безлічі вибрати варіант, найбільш доцільний у заданих умовах?

За якими критеріями слід робити цей вибір?

Принциповий розв’язок цих питань в остаточному підсумку зводиться до оптимізації систем зв’язку за критеріями ефективності.

У загальному випадку результат роботи системи зв’язку визначається кількістю і якістю переданої інформації. Кількість оцінюється швидкістю передачі інформації з каналу Ккан(біт/с), а якість - величиною помилки. Згідно з теоремами К. Шенона, помилка при відповідному виборі методу передачі (модуляції/кодування) може бути зроблена довільно малою. У той самий час швидкість передачі не може бути вище деякого інформаційного ресурсу, називаного пропускною здатністю каналуСк*.*

У сучасних телекомунікаційних системах повсюдно використовуються цифрові методи передачі інформації. Інтенсивне впровадження цифрових технологій обумовлено низкою їх істотних переваг порівняно з аналоговими. Цифрові системи (ЦС) мають більш високу пропускну здатність за умови застосування ефективних методів модуляції/кодування і реалізації оптимальних методів приймання. У ЦС є можливість більш повного використання статистичних характеристик переданих повідомлень.

Цифрова телекомунікаційна система (ЦТКС) — складний комплекс, основним завданням якого є передача інформації із заданими вірністю і швидкістю. Основні вимоги до ЦТКС формулюються досить просто:

* вірність;
* швидкість;
* своєчасністьдоставки інформації від відправника до одержувача.

Процеси, що відбуваються в сучасному світі, все більше демонструють взаємозв’язок і взаємозалежність глобалізації та розвиток інформаційно-ко­мунікаційних технологій. Інформаційні, технологічні інновації та інновації управління істотно розширюють можливості управління державою, розвитку інформаційного обміну, надавання державних послуг, а також підвищують цінність інформації як стратегічного ресурсу.

Разом з розвитком нових технологій і розширенням доступу до інформаційно- комунікаційних систем і технологій (далі - інфокомунікацій) зростають і загрози для інформаційної безпеки (далі - ІБ), від міжнародного тероризму, ризики для розвитку особистості, суспільства і держави.

Заходи щодо забезпечення ІБ і кіберзахисту є основою для конструктивної взаємодії органів державної влади, організацій та громадських об’єднань для захисту національних інтересів і забезпечення безпеки особи, суспільства і держави.

2. ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Процеси, що відбуваються в сучасному світі, все більше демонструють взаємозв’язок і взаємозалежність глобалізації та розвиток інформаційно-комунікаційних технологій. Інформаційні, технологічні інновації та інновації управління істотно розширюють можливості управління державою, розвитку інформаційного обміну, надавання державних послуг, а також підвищують цінність інформації як стратегічного ресурсу.

Разом з розвитком нових технологій і розширенням доступу до інформаційно- комунікаційних систем і технологій (далі - інфокомунікацій) зростають і загрози для інформаційної безпеки (далі - ІБ), від міжнародного тероризму, ризики для розвитку особистості, суспільства і держави.

Заходи щодо забезпечення ІБ і кіберзахисту є основою для конструктивної взаємодії органів державної влади, організацій та громадських об’єднань для захисту національних інтересів і забезпечення безпеки особи, суспільства і держави.

2.1 Еволюція парадигми інформаційної безпеки

Поняття парадигми розглядають як сукупність цінностей, методів, підходів, технічних навичок та засобів, способів розв’язання завдань, прийнятих у науковому співтоваристві фахівців (інформаційної безпеки), в рамках усталеної наукової традиції в певний період часу. Історично парадигми ІБ послідовно змінювали одна одну, зберігаючи, доповнюючи і вдосконалюючи попередні:

- класична парадигма захисту інформації, заснована на контролі доступів;

- парадигма ешелонованої багаторівневої системи ІБ інформаційних ресурсів і технологій (система кругової оборони);

- мережецентрична парадигма ІБ інформаційних ресурсів;

- парадигма кібербезпеки підприємств.

Класична парадигма захисту інформації, заснована на контролі доступів, була застосована до автономної персональної електронної обчислювальної машини (ПЕОМ). Класична парадигма полягає в забезпеченні збереження заданих властивостей інформації та автоматизованої системи, а саме в конфіденційності та цілісності інформації, доступності ресурсу системи, цілісності та спостережності автоматизованої системи [8].

Головною метою системи захисту інформації є попередження загроз безпеці інформації, недопущення крадіжки інформації та комп’ютерних засобів, розголошення, втрати, спотворення і знищення інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об’єкта інформаційної діяльності. Теоретичною базою систем захисту стала теорія гарантовано захищених систем [8]. Загальним принципом діяльності в сфері захисту інформації є максимум ефективності за припустимого ризику не нижче від зафіксованого ризику, коли оперативний ризик є мінімальним.

Класична парадигма захисту інформації була поширена на локальну обчислювальну мережу (ЛОМ), з’єднання між комп’ютерами якої не виходять за межі контрольованої зони. Системи захисту інформації будувалися на основі теорії гарантовано захищених мереж, модель яких містить у собі гарантовано захищені вузли і гарантовано захищені канали, які з’єднують вузли між собою. У комунікаційних системах міжнародними рекомендаціями [5] визначаються такі завдання безпеки мереж зв’язку:

- конфіденційність інформації, яка зберігається або переноситься;

- цілісність даних, тобто інформації, яка зберігається або переноситься;

- цілісність системи, то є завданням захисту операційної системи;

- звітність (до якої входить і завдання спостережності), коли кожен об’єкт/ суб’єкт відповідальний за будь-які дії, які ним ініційовані;

- готовність, за якої всі авторизовані об’єкти повинні отримувати коректний доступ до комунікаційної системи.

Свого найвищого розвитку класична парадигма захисту інформації досягла в автоматизованих системах, в яких інформація передаються через незахищене середовище. На цьому етапі змінилася термінологія: замість терміна «автоматизована система» стали застосовувати більш коректний термін: «інформаційно-телекомунікаційна система» (ІТС).

Адекватний рівень ІБ в ІТС може бути забезпечений лише на основі комплексного підходу, що передбачає планомірне використання фізичних, програмно- технічних та організаційних заходів і засобів. Захисту підлягають усі складові інформаційно-телекомунікаційної системи: лінії, канали, системи передачі, обладнання, програмне забезпечення, інформація і персонал. Із теоретичних положень технічного захисту інформації відомо, що найслабша ланка, яка не блокована організаційними та/або організаційно-технічними або криптографічними засобами, визначає результуючий рівень захищеності.

Парадигма ешелонованого багаторівневого захисту інформаційних ресурсів розвинулася з розширенням сфери застосування інформаційних технологій, глобальним поширенням Інтернету. Передумовами концепції є поява операційних систем з багаторівневим захистом від несанкціонованого доступу, застосування криптографії для шифрування транзакцій, упровадження засобів блокування підключення пристроїв. Характерною особливістю цієї парадигми є перехід від концепцій захисту інформації до концепції ІБ технологій та інформаційних ресурсів. Додатково до головної мети системи ІБ додається забезпечення сталого функціонування ІТС, захист законних інтересів підприємств від протиправних посягань, недопущення крадіжки фінансових коштів, підвищення якості наданих послуг і гарантій безпеки майнових прав та інтересів абонентів. Концептуальна технічна модель ешелонованої багаторівневої системи інформаційної безпеки надана міжнародним стандартом ISO / IEC 15408 [6], який визначає технологію розробки профілів захисту і проектів безпеки [7]. Модель системи ІБ містить у собі набір послуг безпеки, які забезпечують функції моніторингу, захисту та застосування інформаційних ресурсів з метою поетапного запобігання можливості проникнення порушника, виявлення факту проникнення, локалізації об’єкта вторгнення і нападу, нейтралізації і видворення порушника, відновлення втрачених функцій системи. Новим в концептуальній моделі є широке застосування фільтрів, міжмережних екранів, які забезпечують захист периметра. Оскільки близько половини проблем з інформаційною безпекою пов’язано з людським фактором, для захисту від внутрішніх і зовнішніх зловмисників упроваджуються системи виявлення атак, розпізнавання аномальної поведінки, адаптивні алгоритми відновлення систем.

Мережецентрична парадигма ІБ інформаційних ресурсіввипливає із сучасного набутого досвіду і наукових досягнень у цій галузі, бурхливого розвитку ІТС, з розвитку, складності та зростаючої ролі мереж зв’язку як критичного державного ресурсу. Характерною особливістю цієї парадигми є:

дедалі більше переплетіння ІБ з процесами управління комунікаціями: енер­гетичними,

- транспортними, трубопровідними мережами;

- вихід на перший план властивостей доступності та цілісності як показників сталого й ефективного функціонування систем [8].

ІБ телекомунікаційних мереж повинна забезпечуватися за умов інтеграції інформаційних і телекомунікаційних технологій, різноманітних типів мереж і телекомунікаційних послуг, а також дії на мережах операторів різної форми власності. Комплексний підхід означає необхідність створення мережної інфраструктури забезпечення ІБ, оскільки вразливість будь-якої ланки мережі може створити проблеми для провайдерів, операторів, споживачів послуг.

Захист інформації в системах телекомунікацій є складним комплексним завданням. Безпечна телекомунікаційна мережа повинна бути захищена від злочинних і ненавмисних атак, бути надійною, масштабованою, забезпечувати гарантований час відповіді, доступність послуг та інформації, цілісність інформації та обладнання, точність білінгової інформації. ІБ повинна забезпечуватися не тільки від загроз кожного елемента або сервісу, а має бути забезпечена у взаємодії засобів і заходів безпеки в мультимедійному середовищі за цілковитої комплексної реалізації безпеки передачі інформації з кінця в кінець [4].

В ІТС забезпечення інформаційної безпеки тісно інтегрується з такими складовими:

- управління якістю надання послуг зв’язку, де захищеність і готовність інформаційних ресурсів є складовою оцінки якості;

- управління економічною ефективністю, де є взаємозв’язок між інформаційними та економічними ризиками;

- завдання технічної експлуатації щодо забезпечення вимог до збереження мінімального набору критично важливих функцій, до живучості інформаційних систем, до запасу сталості при дії дестабілізуючих факторів зовнішнього середовища.

Сучасна парадигма ІБ, що розвивається у США, розглядає інформаційні системи як принципово відкриті, де синергетика гомеостазу (стан сталої рівноваги) визначається балансом ентропії (мірою невизначеності) зовнішнього середовища і запасом живучості елементів. Парадигма передбачає, перш за все, підвищені вимоги до живучості інформаційних систем, які характеризуються високим ступенем розподілу ресурсів (технічна експлуатація та обслуговування, алгоритми, програмне та апаратне забезпечення, телекомунікації) і децентралізацією управління.

На розвиток моделі ІБ ІТС і мереж зв’язку впливають нові чинники: зростання ролі мереж зв’язку серед критичних фізичних та інформаційних ресурсів держави; особливості функціонування мереж зв’язку, необхідність посиленого розвитку певних функцій і послуг мереж зв’язку у світі впровадження систем електронного уряду, електронного документообігу, електронного цифрового підпису, розвитку електронної торгівлі тощо. Забезпечення ІБ містить у собі такі поняття, як цілісність (integrity) інформації, конфіденційність (confidentiality), захищеність від несанкціонованого доступу (authentication, non-repudiation), забезпечення надійності (availability) системи.

Реалізація сучасної парадигми ІБ, з огляду на всі перелічені фактори, дає гарантію, що навіть при випадковому або зловмисному спотворенні інформації, несанкціонованому проникненні в контур управління, втраті частини ресурсів і перевантаженні трафіка, комплекс організаційно-технічних заходів захисту забезпечить виконання найбільш важливих завдань.

Парадигма кібербезпеки підприємств як розвиток мережецентричної парадигми передбачає перехід від забезпечення інформаційної безпеки технологій до кібербезпеки кіберсередовища та ресурсів організацій і користувачів. Для підприємств ІТС актуальна концепція кібербезпеки.

Кібербезпека(КБ) — це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути застосовані для захисту кіберсередовища, ресурсів організацій та користувача. Ресурси організації або користувача охоплюють приєднані комп’ютерні пристрої, персонал, інфраструктуру, застосування, послуги, системи зв’язку і всю сукупність переданої та/або збереженої інформації в кіберсередовищі. КБ полягає в намаганні досягти і зберегти властивості безпеки у ресурсів організації або користувача, спрямованих проти відповідних загроз безпеки в кіберсередовищі. Загальні завдання забезпечення безпеки містять у собі: доступність; цілісність, яка може охоплювати автентичність і невідновність; конфіденційність.

Кіберсередовищепередбачає користувачів, мережі, пристрої, все програмне забезпечення, процеси, збережену або транзитну інформацію, застосування, послуги і системи, які можуть бути прямо чи опосередковано з’єднані з мережами. До кіберпростіру входять програмне забезпечення, яке працює в комп’ютерних пристроях, інформація, що зберігається (і передається) у цих пристроях або створюється цими пристроями. Обладнання та будівлі, в яких розміщені ці пристрої, також є частиною кіберсередовища.

«У сучасному діловому оточенні концепція периметра зникає. Межі між внутрішніми і зовнішніми мережами стають більш розмитими» [9]. Безпека забезпечується на всіх рівнях телекомунікаційних мереж, мережах доступу, мережному, транспортному рівнях, рівнях управління мережею і надавання послуг.

Кіберзлочинність являє собою реальну загрозу для демократичної стабільності та національної безпеки країни, зачіпаючи найважливіші питання прав людини і верховенства закону.

Боротьба з кіберзлочинністю є найважливішим завданням з огляду на те, що цей різновид злочинності може стати (стає) перешкодою на шляху розвитку нових технологій і в цілому для правової, економічної та громадської безпеки. Загрози віртуальних атак, здатних паралізувати фінансову систему або критичну інфраструктуру всієї країни, стають все реальніше. Тому це питання розглядатиметься як найбільш пріоритетне.

2.2 Проблеми, пов`язані з протидією кіберзлочинності

У зв’язку зі стрімким розвитком інфокомунікацій, глобальним охопленням і транснаціональним характером Інтернету, зростанням швидкості обміну інформацією і необхідністю боротьби зі збільшенням числа і розмаїття загроз (віруси, черв’яки, троянські коні, спуфінг, крадіжка ідентичності, спам та інші форми кібератак) проблеми забезпечення інформаційної і кібербезпеки та протидії кіберзлочинності стали одними з найбільш пріоритетних завдань.

Механізми забезпечення національної кібербезпеки. Забезпечення національної інформаційної та кібербезпеки здійснюється за допомогою впровадження належних заходів щодо захисту критичних і життєво важливих об’єктів інформаційної інфраструктури і комп’ютерних систем та мереж від загроз кібернападів.

Стратегії, що мають на меті забезпечення національної безпеки в кіберпросторі, повинні поступово переходити від традиційних підходів, заснованих на реагуванні, до підходів, які дедалі більшою мірою ґрунтуються на попередженні можливих подій, зменшуючи тим самим періоди вразливості, скорочуючи час реагування і послаблюючи атаки. Запобігання атакам шляхом коригування вразливих систем, встановлення брандмауерів та інших технологій управління доступом, здійснення моніторингу з використанням систем виявлення проникнень і реагування на загрози в режимі реального часу набувають вирішального значення для забезпечення ефективної роботи комп’ютерних систем і мереж.

Загрози, ризики та вразливості. Ресурси, які повинні бути захищені, містять у собі: послуги в галузі зв’язку та комп’ютерних операцій; інформацію та дані, у тому числі програмне забезпечення і дані, пов’язані з послугами забезпечення безпеки; персонал, обладнання і засоби.

Загроза безпеки - це потенційне порушення безпеки. Приклади загроз:

- несанкціоноване розкриття інформації;

- несанкціоноване руйнування або зміна даних, обладнання, інших ресурсів;

- крадіжка, видалення, втрата інформації або інших ресурсів;

- переривання обслуговування або відмова в обслуговуванні;

- видавання себе за допущений об’єкт.

Загрози бувають випадковими або навмисними і можуть бути активними або пасивними. Випадкова загроза - це загроза без будь-якого умисного наміру, як, наприклад, помилка в системі або програмі чи фізичний збій обладнання. Навмисна загроза - це загроза, яка реалізується певним суб’єктом, що чинить навмисну дію. До навмисних загроз належать загрози від простого перегляду з використанням легкодоступних інструментів стеження до витончених спроб порушення захисту з використанням спеціальних знань про систему. Якщо реалізується навмисна загроза, вона називається атакою.

Активна загроза - це загроза, яка призводить до деякої зміни стену або роботи системи, таких, як стирання даних або руйнування обладнання. Пасивна загроза не призводить до зміни стаду.

Прикладом пасивної загрози є перехоплення інформації.

Уразливість захисту являє собою результат помилки або дефекту, якими можна скористатися для порушення системи або інформації, що міститься в ній. Існування уразливості означає можливість реалізації загрози.

Рекомендації МСЕ-Т розрізняють чотири види уразливості:

- уразливість, що залежить від моделі загроз, обумовлена складністю прогнозування майбутніх загроз;

- уразливість, що обумовлена проектом і технічними характеристиками, є наслідком помилок та упущень при розробці системи або протоколу, які роблять їх уразливими за визначенням;

- уразливість реалізації являє собою уразливість, що виникає внаслідок помилок в процесі реалізації системи або протоколу;

- уразливість експлуатації та конфігурації виникає внаслідок неналежного використання варіантів при реалізації або неправильної політики та практики впровадження, наприклад: незастосування шифрування в бездротовій мережі.

Ризик порушення безпеки є показником негативних наслідків, які можуть настати, якщо скористатися уразливістю захисту, тобто якщо буде реалізована загроза. Хоча ризик неможливо цілком усунути, однією з цілей захисту є зменшення ризику до прийнятного рівня.

Хоча загрози і фактори загроз змінюються, уразливість захисту буде існувати протягом всього терміну експлуатації системи або протоколу, якщо не вжити конкретних заходів щодо усунення уразливості. Ризики порушення безпеки, зумовлені властивостями протоколу, в разі стандартизованих протоколів можуть бути досить істотними і глобальними за масштабом. Тому важливо зрозуміти і виявити уразливість протоколів та вжити заходів щодо усунення уразливих елементів при їх виявленні.

Організаційні заходи. Для ефективного вирішення питань і безпосереднього виконання функцій щодо забезпечення кібербезпеки в системі виконавчої влади утворюються (створюються) організаційні структури, відповідальні за кібербезпеку та кіберзахист у державі, що займаються системами спостереження й оповіщення та реагують на інциденти, а також організаційні структури для координації діяль­ності з реагування на кібератаки. Якщо кібератака відбувається в одній країні, її руйнівні наслідки можуть протягом декількох хвилин досягти своїх жертв у країнах, між якими є з’єднання. Вільний потік інформації, спільна робота та співпраця між національними організаційними структурами мають життєво важливе значення для ефективного усунення таких інцидентів і реагування на них.

Деякі можливі компоненти такої структури можуть містити:

- національний координатор з питань кібербезпеки, до завдання якого буде входити організація роботи та координація зусиль, взаємодія з урядом, представниками ділових кіл та наукового співтовариства;

- можливості щодо усунення інцидентів з відповідальністю на державному рівні. Ця діяльність повинна передбачати можливе створення Національного центру кібербезпеки з метою установи в середньостроковій/довгостроковій перспективі спеціальних груп CERT/CSIRT.

Для органів державного управління важливо створити або визначити національну організацію (національний центр кіберзахисту) зі статусом первинної ланки, яка була б координуючим органом для забезпечення безпеки кіберпростору та захисту найважливішої інформаційної інфраструктури, основним завданням якою була б діяльність із спостереження, попередження, реагування та відновлення, а також сприяння співробітництву між урядовими органами, приватним сектором, науковими колами та міжнародним співтовариством. Слід передбачити заходи щодо посилення можливостей антикризового реагування в разі катастроф та надзвичайних ситуацій. Доцільно створити національний координаційний орган, відповідальний за збір, аналіз та зберігання статистичної інформації про всі правопорушення (інциденти) у сфері кібербезпеки, у тому числі і про ті, що стосуються поширення та масштабів кіберзлочинності для розробки рекомендацій.

Потрібно створити і впровадити механізм з надання зрозумілих правил щодо того, як повідомляти про незаконний контент, виявлений у мережі Internet (наприклад, державна гаряча лінія, яка має можливість швидкого реагування та видалення незаконного матеріалу або заборони доступу до нього); посилити роль регуляторних органів та уповноважити їх взяти на себе завдання моніторингу діяльності, наприклад, за допомогою груп реагування на комп’ютерні інциденти (CIRT) або груп реагування на порушення комп’ютерного захисту (CERT).

Сучасні методи забезпечення кібербезпеки містять у собі:

- криптографію: ця потужна технологія підтримує низку послуг безпеки, у тому числі шифрування даних при передачі та під час зберігання;

- контроль за доступом - для обмеження можливості користувачів у доступі, перегляді або зміні інформації в головних комп’ютерах або мережах;

- технічний захист інформації: завдання полягає в недопущенні витоку інформації технічними каналами; у запобіганні зовнішнього впливу на інформацію, обладнання та інші ресурси, забезпечення фізичного захисту інформаційних ресурсів і кіберсередовища від несанкціонованого доступу

- цілісність системи — для того, щоб система та її дані не були змінені або спотворені неуповноваженими сторонами чи несанкціонованим чином;

- аудит, реєстрацію та моніторинг: допомагає системним адміністраторам збирати й аналізувати мережні журнали під час і після зловмисних дій. Дані можуть використовуватися для оцінки ефективності стратегії безпеки;

- управління безпекою: забезпечується і допомагає системним адміністраторам при аналізі та налаштуванні параметрів безпеки на їх головних комп’ютерах і мережах. Адміністративний контроль може використовуватися для перевірки точності функціонування мережі та підключення установки елементів. Керівництвом для розробки всеосяжної політики в галузі безпеки, планів реагування на інциденти та відновлення може служити Архітектура, передбачена в Рекомендації МСЕ-Т Х.805.

Захист дітей в онлайновому середовищі (заходи щодо посилення захисту дітей). Захист дітей в онлайновому середовищі передбачає створення технічних механізмів, що мають на меті зменшення ризиків для дітей та молоді, які працюють в онлайновому режимі, передаючи:

- розробку механізмів автентифікації і авторизації для забезпечення захисту дітей від неналежного матеріалу;

- розробку міжнародно визнаної бази даних для правоохоронних органів;

- розроблення та впровадження національної стратегії (концепції), спрямованої на безпеку дітей в онлайновому режимі.

3. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Технічний захист інформації (ТЗІ) — це вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [10]. Він реалізується системою ТЗІ, яка згідно з державним стандартом [11] є сукупністю організаційних структур, нормативно-правових документів та матеріально-технічної бази. Системи складаються з технічних засобів, організаційних заходів захисту та криптографічних засобів. Криптографічні заходи мають тут обмежене, але невід’ємне застосування - для захисту інформації, що зберігається на носіях та передається каналами зв’язку між елементами інформаційної системи. Серед організаційних засобів захисту істотну роль відіграють механізми захисту, які пов’язані з персоналом.

3.1. Класифікація технічних каналів витоку інформації

Технічний канал витоку інформації - це сукупність об’єкта розвідки, технічного засобу розвідки, за допомогою якого добувається інформація про цей об’єкт, і фізичного середовища, в якому поширюється інформаційний сигнал. Класифікацію технічних каналів витоку показано на рис. 3.1.

Сигнали є матеріальними носіями інформації. За своєю фізичною природою сигнали можуть бути електричними, електромагнітними, акустичними та ін. Тобто сигналами, як правило, є електричні, електромагнітні, механічні та інші види коливань (хвиль), причому інформація утримується в їх змінюваних параметрах. Залежно від природи сигнали поширюються в певних фізичних середовищах. У загальному випадку середовищем поширення можуть бути газові (повітряні), рідинні (водні) та тверді середовища. Наприклад, повітряний простір, конструкції будинків, з’єднувальні лінії та струмопровідні елементи, ґрунт (земля) тощо.

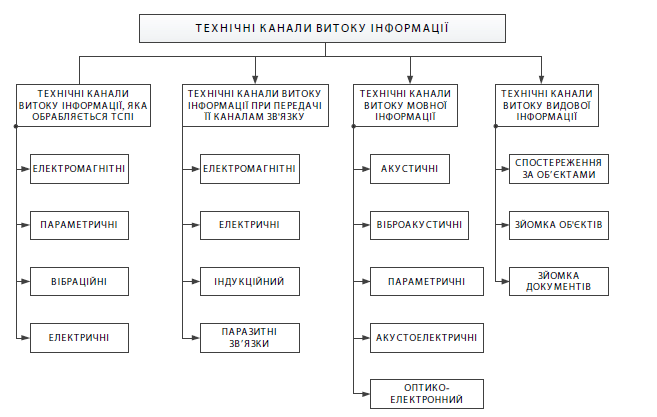


Рис. 3.1 Класифікація технічних каналів витоку інформації

Під акустичною мається на увазі інформація, носієм якої є акустичні сигнали. Якщо джерелом інформації є людське мовлення, акустична інформація називається мовною. Акустичний сигнал являє собою збурювання пружного середовища, що виявляється у виникненні акустичних коливань різної форми та тривалості. Акустичними називаються механічні коливання часток пружного середовища, що поширюються від джерела коливань у навколишній простір у вигляді хвиль різної довжини.

Первинними джерелами акустичних коливань є механічні коливальні системи, наприклад органи мовлення людини, а вторинними - перетворювачі різного типу, у тому числі електроакустичні. Останні являють собою пристрої, які призначені для перетворювання акустичних коливань на електричні та навпаки. До них належать п’єзоелементи, мікрофони, телефони, гучномовці та інші пристрої. Залежно від форми акустичних коливань розрізнюють прості (тональні) та складні сигнали. Тональний - це сигнал, спричинюваний коливанням, що відбувається за синусоїдальним законом. Складний сигнал містить цілий спектр гармонічних складових. Мовний сигнал є складним акустичним сигналом у діапазоні частот від 200...300 Гц до 4...6 кГц.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їх перехоплювання технічні канали витоку акустичної (мовної) інформації можна розподілити на повітряні, вібраційні, електроакустичні, електричні, електромагнітні, оптикоелектронні та параметричні.

Найчастіше канали витоку виникають за рахунок технічних засобів приймання, опрацьовування, зберігання та передавання інформації, які безпосередньо опрацьовують конфіденційну інформацію. До таких засобів належать: електронно- обчислювальна техніка, режимні АТС, системи оперативно-командного й гучномовного зв’язку, системи звукопідсилювання, звукового супроводження й звукозапису тощо.

При виявленні технічних каналів витоку опрацьовування, зберігання й передавання інформації необхідно розглядати як систему, яка містить основне (стаціонарне) обладнання, прикінцеве обладнання, з’єднувальні лінії (сукупність проводів і кабелів, прокладених поміж окремими технічними засобами прийому, опрацьовування, зберігання й передачі інформації та їх елементами), розподільне й комутаційне обладнання, системи електроживлення, системи заземлення.

Окремі технічні засоби чи група технічних засобів, призначених для опрацьовування конфіденційної інформації, разом із приміщеннями, в яких вони розміщуються, становлять об’єкт інформаційної діяльності. Під об’єктами інформаційної діяльності розуміють також виділені приміщення, які слугують для проведення закритих заходів.

Поряд з технічними засобами приймання, опрацьовування, зберігання й передавання інформації в приміщеннях встановлюються технічні засоби та системи, які безпосередньо не беруть участі в опрацьовуванні конфіденційної інформації, але використовуються разом з технічними засобами приймання, опрацьовування, зберігання та передавання інформації та перебувають у зоні електромагнітного поля, яке ними створюється. Такі технічні засоби і системи є допоміжними технічними засобами та системами. До них належать: технічні засоби відкритого телефонного, гучномовного зв’язку, системи пожежної й охоронної сигналізації, електрифікації, радіофікації, часофікації, електропобутові прилади тощо.

Окрім з’єднувальних ліній технічних засобів приймання, опрацьовування, зберігання й передавання інформації та допоміжних технічних засобів і систем, за межі контрольованої зони можуть виходити проводи та кабелі, які до них не належать, але проходять через приміщення, де встановлено технічні засоби, а також металеві труби систем опалення, водозабезпечення й інші струмопровідні металоконструкції. Такі проводи, кабелі та струмопровідні елементи називають сторонніми провідниками.

Повітряні технічні канали витоку інформації.У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, і для їх перехоплення використовуються мініатюрні високочутливі мікрофони та спеціальні спрямовувальні мікрофони.

Як можливі канали витоку інформації найбільший інтерес являють допоміжні технічні засоби та системи, котрі мають вихід за межі зони, яка контролюється, тобто зони, в якій унеможливлене неконтрольоване з’явлення осіб та транспортних засобів, які не мають постійних чи тимчасових перепусток

Вібраційні технічні канали витоку інформації. У вібраційних технічних каналах витоку інформації середовищем поширення акустичних сигналів можуть бути конструкції будинків, споруд (стіни, стелі, підлоги), труби водопостачання, опалення, каналізації, вентиляційні канали. Для перехоплення акустичних коливань у цьому разі використовуються контактні мікрофони (стетоскопи). Контактні мікрофони, з’єднані з електронним підсилювачем, називають електронними стетоскопами. На вібраційному каналі також можливе перехоплення інформації з використанням закладних пристроїв. Переважно для передавання інформації використовується радіоканал, тому такі пристрої часто називають радіостетоскопами. Можливе використання закладних пристроїв з передаванням інформації з оптичного каналу в близькому інфрачервоному діапазоні довжин хвиль, а також з ультразвуковим каналом

Електроакустичні технічні канали витоку інформації.Електроакустичні технічні канали витоку інформації виникають унаслідок електроакустичних перетворень акустичних сигналів на електричні та містять у собі перехоплення акустичних коливань технічними засобами й системами, яким притаманний «мікрофонний ефект», а також шляхом «високочастотного нав’язування».

Деякі елементи допоміжних технічних засобів та систем, у тому числі трансформатори, котушки індуктивності, електромагніти вторинних електрогодинників, дзвінки телефонних апаратів, дроселі ламп денного світла, електрореле й т.ін., мають властивість змінювати свої параметри (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом акустичних коливань. Змінювання параметрів призводить або до виникнення на цих елементах електрорушійної сили, яка змінюється за законом змінювання впливаючого інформаційного акустичного поля, або до модуляції струмів, що протікають цими елементами, інформаційним сигналом. Наприклад, акустичне поле, впливаючи на якір електромагніта викличного телефонного дзвінка, спричинює його коливання. Внаслідок цього змінюється магнітний потік осердя електромагніту. Змінювання цього потоку спричинює виникнення електрорушійної сили самоіндукції в котушці дзвінка, яка змінюється за законом змінювання акустичного поля.

Допоміжні технічні засоби та системи, окрім зазначених елементів, можуть містити безпосередньо електроакустичні перетворювачі. До таких засобів і систем належать деякі датчики пожежної сигналізації, гучномовці ретрансляційної мережі тощо. Нагадаємо, що ефект електроакустичного перетворення акустичних коливань на електричні часто називають «мікрофонним ефектом». Найбільшу чутливість до акустичного поля мають абонентські гучномовці й деякі датчики пожежної сигналізації.

Перехоплення акустичних коливань у певному каналі витоку інформації здійснюється шляхом безпосереднього приєднування до з’єднувальних ліній допоміжних технічних засобів та систем, яким притаманний «мікрофонний ефект», спеціальних високочутливих низькочастотних підсилювачів. Наприклад, приєднуючи такі засоби до з’єднувальних ліній телефонних апаратів з електромеханічними викличними дзвінками, можна прослуховувати розмови, що відбуваються в приміщеннях, де встановлено ці апарати.

Електричні канали витоку інформації. Причинами виникнення електричних каналів утрати інформації можуть бути:

- наведення електромагнітних випромінювань технічних засобів обробки інформації на з’єднувальні лінії допоміжних технічних засобів і систем та сторонні провідники, які виходять за межі контрольованої зони;

- просочування інформації колами електроживлення технічних засобів приймання, опрацювання, зберігання та передавання інформації;

- просочування інформаційних сигналів у колах заземлення технічних засобів приймання, опрацьовування, зберігання й передавання інформації.

Електромагнітні канали витоку інформації. До електромагнітних каналів витоку інформації належать канали, які виникають через різноманітні сторонні електромагнітні випромінювання технічних засобів приймання, опрацювання, зберігання, передавання (далі - обробки) інформації:

- випромінювання елементів технічних засобів обробки інформації;

- випромінювання на частотах роботи генераторів обробки інформації;

- випромінювання на частотах самозбудження підсилювачів низької частоти технічних засобів обробки інформації.

Оптикоелектронні технічні канали витоку інформації. Оптикоелектронні (лазерні) канали витоку акустичної інформації утворюються при опроміненні лазерним променем вібруючих в акустичному полі тонких відбивальних поверхонь (шибок вікон, картин, дзеркал тощо). Відбите лазерне випромінювання (дифузійне чи дзеркальне) модулюється за амплітудою та фазою (за законом вібрації поверхні) і приймається приймачем оптичного (лазерного) випромінювання, за демодуляції якого виокремлюється мовна інформація. Причому лазер та приймач оптичного випромінювання можуть бути встановлені в одному чи різних місцях (приміщеннях).

Для перехоплення мовної інформації з каналу використовуються складні лазерні акустичні локаційні системи, які іноді називають «лазерними мікрофонами». Працюють вони у близькому інфрачервоному діапазоні хвиль.

3.2 Засоби виявлення технічних каналів витоку

Принцип дії більшості індикаторів електромагнітного поля заснований на широкосмуговому детектуванні електричного поля. Індикатори забезпечують можливість виявлення радіопередавальних прослуховуючих пристроїв з будь-якими видами модуляції. Багато комплексів для проведення спецдосліджень дозволяють в автоматичному режимі розв’язувати низку завдань вимірювань ПЕМВН і полегшують роботу інженера-дослідника.

Деякі комплекси на основі скануючих приймачів або аналізаторів спектра застосовуються для швидкого аналізу спектра ПЕМВН, випромінюваних технічним засобом, але не забезпечують високої точності вимірювань. У разі потреби видачі припису на експлуатацію технічного засобу вимірювання, проведені за допомогою таких комплексів, підлягають обов’язковій ручній перевірці з використанням метрологічного вимірювального обладнання (вимірювальних приймачів або аналізаторів спектра).

Автоматизація виявлення гармонічних складових тестового сигналу. Зазвичай інженер-дослідник шукає гармонічні складові «на слух», розпізнаваючи розшукувані компоненти за звуком і формою осцилограми демодульованого сигналу. Інструментальна реалізація такого режиму призводить до того, що автоматична система, яка розпізнає сигнали за їх формою, працює не набагато швидше кваліфікованого інженера-дослідника. Тому в перших комплексах цей режим не було реалізовано, а впізнання проводилося за критерієм зміни рівнів сигналів при включенні тестового режиму на досліджуваному технічному засобі (так званий «енергетичний критерій»). Такий спосіб дає непогані результати: вся робота з виявлення зводиться до двох проходів сканування діапазону спецдосліджень: при першому проході запам’ятовується картина шумів у вимкненому тестовому режимі, при другому проході досліджуваний технічний засіб переводиться в тестовий режим, і вимірюються рівні всіх сигналів, що перевищують запам’ятовані шуми на задане значення порогу. Прискорення роботи досягається дуже істотне: замість кількох годин спецдослідження виконується за лічені хвилини. У результаті інженер-дослідник отримує таблицю частот і рівнів сигналів (типова кількість виявлених складових - декілька сотень) і можливість розрахувати зони розвіддоступності. Однак результати розрахунку можуть виявитися невірними, оскільки електромагнітний стан змінюється з часом. У діапазоні від 9 кГц до 1000 МГц працюють тисячі радіостанцій і джерел радіоперешкод. Деякі з них час від часу вмикаються і вимикаються, і якщо якесь джерело радіовипромінювання не працювало під час сканування спектра шумів, а при другому проході увімкнулось, його частота виявиться у списку виявлених складових. Звичайно, це може випадково змінити розраховані розміри зон розвіддоступності. Операторові доводиться вручну перевіряти всі виявлені складові, на що буде витрачено час.

У більш досконалих комплексах застосовується автоматичне розпізнавання інформаційних сигналів. Згідно з методикою інженеру-досліднику пропонується виконати пошук будь-якої гармонічної складової вручну чи в спеціальному «напівавтоматичному» режимі або створити еталонний образ шуканого сигналу за допомогою редактора (генератора), або обрати раніше створений образ із бібліотеки, після чого комплекс автоматично виявляє в ефірі сигнали, схожі на заданий сигнал. Для впізнання сигналів у таких комплексах застосовується взаємно кореляційна функція. Це більше витратний за часом спосіб, але й істотно більш точний.

Вимірювання наведень у мережі живлення, лініях і комунікаціях. Згідно з чинними нормативними документами, вимірювання наведень у мережі живлення повинно здійснюватися за допомогою еквівалента мережі або пробників напруги. Еквівалент мережі досить складний і порівняно дорогий пристрій, однак вимірю­вання, проведені за його допомогою, зазвичай точніші вимірювань, виконаних за допомогою пробника напруги. «Чиста» мережа, імітована еквівалентом мережі, дозволяє вимірювати створювані досліджуваним технічним засобом наведення в мережу живлення, рівень яких на 4 - 6 дБ вище власних шумів еквівалента мережі, тоді як точність вимірювань, що виконуються за допомогою пробника напруги, залежить від рівнів шуму мережі живлення. Для автоматизованих вимірювальних систем дуже важлива можливість використання у своєму складі різних приймальних пристроїв: антен, пробників напруги, еквівалентів мережі.

Відповідно в програмному забезпеченні комплексу повинен бути передбачений механізм підтримки додаткових приймальних пристроїв, а саме можливість уведення таких параметрів, як робочий діапазон, антенні коефіцієнти (коефіцієнти загасання або посилення) та їх автоматичний облік у процесі вимірювань.

Особливості функціонування різного роду технічних засобів радіомоніторингу та виявлення закладних пристроїв розглянемо на конкретних прикладах їх технічної реалізації.

Слід наголосити на ефективному використанні досить простих і недорогих багатофункціональних комплектів для виявлення каналів витоку інформації, таких, наприклад, як «ПКУ-6М» і «Піранья». Для виявлення технічних каналів витоку інформації широко застосовують доглядові пристрої, такі, як металодетектори, різноманітні ендоскопи, рентгенотелевізійні установки.

Сфера застосування металодетекторів (металошукачів, металовиявлювачів), що дозволяють реєструвати заборонені та небезпечні металеві предмети у непровідному середовищі, весь час розширюється. Останнім часом актуальною стало завдання оснащення металодетекторами таких суто цивільних об’єктів, як школи, лікарні, театри тощо.

Металодетектори застосовуються сьогодні також у дефектоскопії (пошук металевих включень у різних матеріалах), рудний електророзвідці, у системах контролю доступу, запобігання розкраданням тощо.

Портативні рентіенотелевізійні установки застосовуються для проведення заходів щодо виявлення вибухових пристроїв у надісланих згортках, сумках, ручній поклажі, багажі, а також для пошуку приховано встановлених засобів знімання інформації в предметах інтер’єру і меблів, різних побутових приладах.

Ендоскопи призначені для огляду важкодоступних місць у будівельних конструкціях, транспортних засобах, контейнерах, вузлах технологічного устаткування тощо з метою виявлення вибухових пристроїв, зброї, контрабанди, а також негласно встановлених засобів знімання інформації. Спеціальне покриття робочої частини дозволяє обстежити вміст судин з агресивними рідинами, наприклад бензобаки. Ендоскопи можуть комплектуватися мережними освітлювачами (потужністю 100 ВА) і фототелевізійним трактом, що дозволяє отримати високоякісне зображення спостережуваного об’єкта на екрані дисплея.

До сучасного автоматизованого пошуково-вимірювального обладнання належить АКОР ЗПК - автоматизований комплекс радіомоніторингу та пошуку закладних пристроїв, виявлення та вимірювання ПЕМВН від засобів ЕОТ, оргтехніки та пристроїв зв’язку . Комплекс складається із скануючого приймача АР3000, ноутбука, антен, мікрофонів, фільтрів тощо та програмного забезпечення.

Функції комплексу:

- перевірка и контроль приміщень, електромережі, телефонних ліній та офісної техніки на наявність пристроїв негласного знімання мовної інформації, відеокамер та інфрачервоних передавачів (заставних пристроїв);

- виявлення каналів витоку інформації, що передається радіоефіром (радіостанції, телефони стільникового зв’язку стандартів GSM 900/1800, CDMA, DECT;

- систем передачі даних 3G, Bluetooth, Wi-Fi, WiMAX та інших засобів зв’язку), акустичними та віброакустичними каналами;

- виявлення і вимірювання побічних електромагнітних випромінювань і наведень (ПЕМВН) від персональних комп’ютерів (ПК), оргтехніки, апаратури зв’язку та засобів телекомунікацій;

- знаходження серед виявлених ПЕМВН інформативних сигналів та оцінка можливості їх перехоплення.

4. КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Технічний захист інформації можуть здійснювати будь-які організації та підприємства, яким такий захист потрібен. На відміну від цього, згідно з законодавчими та нормативними документами України та інших держав, криптографічний захист інформації (КЗІ) можуть здійснювати лише державні організації та підприємства або інші за їх дорученням. Але за умов всебічного поширення інформаційних технологій та вступу людства у стадію становлення інформаційного суспільства коло застосування КЗІ закономірно розширилось. КЗІ обслуговує сфери бізнесу, банківських послуг, електронної торгівлі, інформаційних технологій, хмарних обчислень та мільярди «звичайних» людей, які починають жити в «електронному» суспільстві.

Криптографічний захист інформації (КЗІ) - це вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховання/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо [13]. Система КЗІ складається із власне криптографічних засобів, технічних засобів для захисту від витоку інформації до шифрування та після дешифрування, організаційних заходів щодо захисту від загроз людських факторів, а також правового, методичного, математичного, програмно-алгоритмічного, інформаційного забезпечень, які попереджують реалізацію загроз або істотно утруднюють реалізацію атак.

Цілі КЗІ випливають із поняття криптографії. Криптографія як теорія є ме­тодологічною основою сучасних систем забезпечення безпеки інформації в інформаційно-комунікаційних системах. Криптографія як технологія являє собою сукупність методів перетворення даних, орієнтованих на те, щоб захистити ці дані, зробити їх некорисними для незаконних користувачів [14]. Такі перетворення забезпечують вирішення трьох проблем захисту даних: гарантію конфіденційності, цілісності та автентичності даних, які передаються чи зберігаються.

Завдання КЗІ. Для забезпечення безпеки даних необхідно підтримувати розв’язання трьох основних завдань:

- забезпечення конфіденційності даних, що передаються або зберігаються;

- підтвердження цілісності та автентичності даних;

- автентифікація абонентів при вході в систему та при з’єднанні.

Для реалізації цих завдань використовуються криптографічні технології шифрування, автентифікації та цифрового підпису. Конфіденційність забезпечується за допомогою алгоритмів та методів шифрування, а також шляхом взаємної автентифікації абонентів на основі багаторазових чи одноразових паролів, цифрових сертифікатів, флеш-карт тощо. Цілісність та автентичність даних, що передаються, зазвичай досягаються за допомогою технології цифрового підпису. Автентичність дозволяє встановлювати з’єднання лише між легальними користувачами та попереджує доступ до телекомунікаційних послуг небажаних осіб.

КЗІ застосовується для захисту інформації, яка передається каналами зв’язку або зберігається в базах даних, робочих станціях, міститься у парольних та ключових даних систем автентифікації та розмежування доступу.

4.1 Криптографічні засоби захисту

Узагальнену модель криптографічної системи, що забезпечує шифрування переданої інформації, показано на рис. 4.1. Відправник генерує відкритий текст вихідного повідомлення Р, яке повинно бути передане адресату незахищеним каналом. За каналом стежить перехоплювач (зловмисник) з метою перехопити і розкрити передане повідомлення. Для того щоб перехоплювач не зміг дізнатися змісту повідомлення Р, відправник шифрує його за допомогою оборотного перетворення Ек і отримує шифротекст (криптограму) С = Ек(Р), який відправляє адресату. Адресат, прийнявши шифротекст С, розшифровує його за допомогою зворотного перетворення Б = Е-1к і отримує вихідне повідомлення у вигляді відкритого тексту Р: Бк (С) = Е-1к (Ек (Р) = Р.

Перетворення Ек вибирається з сімейства криптографічних перетворень, які називаються криптоалгоритмами. Параметр, за допомогою якого вибирається певне перетворення, що використовується, називається криптографічним ключем К. Криптосистема має різні варіанти реалізації: набір інструкцій, апаратні засоби, комплекс програм комп’ютера, які дозволяють зашифрувати відкритий текст і розшифрувати шифртекст різними способами, один з яких вибирається за допомогою конкретного ключа К. Параметр К (ключ) обирається з кінцевої множини К, яка називається простором ключів.

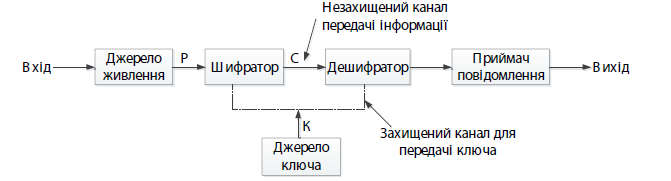


Рис. 4.1 Модель криптографічної системи

У загальному випадку перетворення шифрування може бути симетричним або асиметричним щодо перетворення розшифрування. Ця важлива властивість функції перетворення визначає два класи криптосистем:

- симетричні (одноключові) криптосистеми;

- асиметричні (двохключові) криптосистеми (з відкритим ключем).

Схема симетричної криптосистеми з одним секретним ключем показана на рис. 4.1. У ній використовуються однакові секретні ключі в блоці шифрування і блоці розшифрування. В асиметричній криптосистемі з двома різними ключами один із ключів відкритий, а інший — секретний.

У симетричній криптосистемі секретний ключ треба передавати відправникові та одержувачеві захищеним каналом розповсюдження ключів, наприклад такому, як кур’єрська служба. На рис. 4.1 цей канал позначений пунктирними лініями. Існують і інші способи розподілу секретних ключів. В асиметричній криптосистемі передають незахищеним каналом тільки відкритий ключ, а секретний ключ зберігають на місці його генерації.

Оскільки між шифратором і дешифратором передача інформації здійснюється незахищеним каналом, перехоплювач може застосувати активні дії, які полягають не тільки у зчитуванні всіх шифротекстів, переданих каналом, а також у спробі зміни їх на свій розсуд. Будь-яка спроба з боку перехоплювача розшифрувати шифртекст С для отримання відкритого тексту Р або зашифрувати свій власний текст М' для отримання правдоподібного шифротексту С', не маючи справжнього ключа, називається криптоаналітичною атакою. Якщо вжиті криптоаналітичні атаки не досягають мети і криптоаналітик не може, не маючи справжнього ключа, вивести Р з С або С' з М', то вважають, що така криптосистема є криптостійкою.

Криптоаналіз *-* це наука про розкриття вихідного тексту зашифрованого повідомлення без доступу до ключа. Успішний аналіз може розкрити вихідний текст або ключ. Він дозволяє також виявити слабкі місця в криптосистемі, що, в остаточному підсумку, веде до тих самих результатів. Фундаментальне правило криптоаналізу, вперше сформульоване голландцем А. Керкхоффом ще в ХІХ столітті, полягає в тому, що стійкість шифру (криптосистеми) повинна визначатися тільки секретністю ключа. Іншими словами, правило Керкхоффа полягає в тому, що весь алгоритм шифрування, крім значення секретного ключа, відомий криптоаналітику противника. Це обумовлено тим, що криптосистема, що реалізує сімейство криптографічних перетворень, зазвичай розглядається як відкрита система. Такий підхід відображає дуже важливий принцип технології захисту інформації: захищеність системи не повинна залежати від секретності чогось такого, що неможливо швидко змінити в разі витоку секретної інформації. Зазвичай криптосисте­ма являє собою сукупність апаратних і програмних засобів, яку можна змінити лише за умов великих витрат часу і коштів, тоді як ключ є легко змінним об’єктом. Саме тому стійкість криптосистеми визначається тільки секретністю ключа.

4.2 Класифікація криптоалгоритмів захисту інформації

Відомо декілька класифікацій криптографічних алгоритмів [15]. Одна з них поділяє КА залежно від числа ключів, що застосовуються в конкретному алгоритмі: безключові КА - не використовують в обчисленнях жодних ключів; одноключові КА - працюють з одним ключовим параметром (секретним ключем); двохключові КА- на різних стадіях роботи в них застосовуються два ключових параметри: секретний і відкритий ключі.

Перетворення шифрування може бути симетричним або асиметричним щодо перетворення розшифрування. Відповідно, розрізняють два основні класи криптосистем: симетричні криптосистеми та асиметричні криптосистеми.

Існують більш детальні класифікації, наприклад, показана на рис. 4.2.

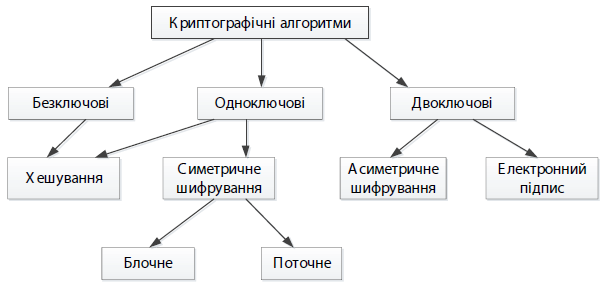


Рис. 4.2 Класифікація криптоалгоритмів захисту інформації

Хешування - це метод криптозахисту, що являє собою контрольне перетворення інформації: з даних необмеженого розміру шляхом виконання криптографічних перетворень обчислюється хеш-значенчя фіксованої довжини, однозначно відповідне вихідним даним. Хешування може виконуватисі як з використанням деякого секретного ключа, так і без нього. Таке криптографічне контрольне підсумовування широко використовується в різних методах захисту інформації, зокрема, для підтвердження цілісності даних, якщо використання цифрового підпису неможливе (наприклад, через велику ресурсоємність) або надлишкове. Крім того, даний метод застосовується в схемах електронного підпису («підписується» зазвичай хеш-значення даних, а не всі дані цілком), а також у схемах автентифікації користувачів (при перевірці, чи насправді користувач є тим, за кого себе видає).

Симетричне шифрування використовує той самий ключ як для шифрування, так і для розшифрування інформації. Фактично обидва ключі (зашифрування і розшифрування) можуть і різнитися, але якщо в якомусь КА їх легко обчислити один з одного в обидві сторони, такий алгоритм належить до симетричного шифрування. Симетричне шифрування підрозділяється на два види: блочне і поточне. У деяких класифікаціях вони не поділяються. Тоді поточне шифрування - це шифрування блоків одиничної довжини.

Блочне шифрування характеризується тим, що інформація попередньо розбивається на блоки фіксованої довжини (наприклад, 64 або 128 біт). При цьому в різних КА або різних режимах роботи алгоритму блоки можуть шифруватися як незалежно один від одного, так і зі «зчепленням» — коли результат шифрування поточного блоку даних залежить від значення попереднього блоку або від результату шифрування попереднього блоку.

Поточне шифрування застосовується, насамперед, тоді, коли інформацію неможливо розбити на блоки. Скажімо, є якийсь потік даних, кожен символ яких потрібно зашифрувати і відправити, не чекаючи інших даних, достатніх для формування блоку. Алгоритми поточного шифрування шифрують дані побітово або посимвольно.

Асиметричне шифрування характеризується застосуванням двох типів ключів: відкритого - для зашифрування інформації і секретного - для її розшифрування. Секретний і відкритий ключі пов’язані між собою досить складним співвідношенням. Головне в цьому співвідношенні - легкість обчислення відкритого ключа із секретного і неможливість (за обмежений час при реальних ресурсах) обчислення секретного ключа з відкритого при досить великій розмірності операндів.

Електронний цифровий підпис (ЕЦП)використовується для підтвердження цілісності та авторства даних. Як і у випадку асиметричного шифрування, в цьому методі застосовуються двоключові алгоритми з таким самим простим обчисленням відкритого ключа із секретною та практичною неможливістю зворотного обчислення. Однак призначення ключів ЕЦП зовсім інше. Секретний ключ застосовується для обчислення ЕЦП, відкритий ключ необхідний для її перевірки. При дотриманні правил безпечного зберігання безпечного ключа ніхто, крім його власника, не в змозі обчислити вірний ЕЦП будь-якого електронного документа.

4.3 Криптографічні системи з абсолютною стійкістю

Алгоритм шифрування (або шифр) - це переклад відкритого тексту на текст зашифрований (або шифротекст, шифрограму, криптограму) за допомогою секретного ключа. Цей процес називають шифруванням.

С = Ек(m) (4.1)

де – m – відкритий текст, к – секретний ключ, Е – функція, яка шиифрє, С – шифротекст.

Зворотній процес називається розшифруванням:

m= Dk(c) (4.2)

Зауважимо, що алгоритми шифрування і розшифрування Е і Бвідкриті, і таємність вихідного тексту т в цьому шифротексті С залежить від таємності ключа к. Обидві частини цього процесу використовують той самий ключ, у зв’язку з чим такі алгоритми заведено називати симетричними криптосистемами, або криптосистемами із секретним ключем. Існують алгоритми шифрування, що залежать від двох різних ключів. Перший з них відкритий і потрібен для шифрування, тоді як другий - секретний і вживається при відновленні тексту із шифровки. Ці останні криптосистеми називаються асиметричними, або криптосистемами з відкритим ключем.

Криптографічна система називається обчислювально-захищеною (або обчислювально-стійкою), якщо найкращий з можливих алгоритмів, який зламує її, вимагає невиправдано високих витрат обчислювальних ресурсів. Беручи до уваги потужність сучасних комп’ютерів, можна вважати, що 280 операції, необхідних для злому шифру, це та межа, виходячи за яку, алгоритми злому стають занадто дорогими. Таким чином, якщо мінімальне число N операцій, необхідних алгоритму, який атакує криптосистему, більше 280, то говорять, що вона обчислювально захищена.

Практичний підхід, пов’язаний з обчислювальною захищеністю, полягає в тому, щоб звести злом системи до вирішення добре вивчених важких проблем. Наприклад, ми можемо спробувати показати, що розкриття конкретної криптосистеми рівнозначне розкладанню великого цілого числа на множники. Такі системи часто називають доказово стійкими. Однак при цьому стійкість системи обґрунтовується зведенням до важкої задачі, що не можна вважати коректним доказом. За сутністю можна довести, що стала криптографічна система є сталою стосовно противника, чиї обчислювальні ресурси обмежені. Навіть і тоді, коли противник володіє великими, але обмеженими ресурсами, він все ще не зможе зламати систему [16]. Це означає, що в еру надшвидкісних квантових комп’ютерів будуть застосовуватися певні стійкі криптографічні системи.

З іншого боку, система називається абсолютно стійкою, або досконалою, якщо ми не обмежуємо обчислювальної потужності противника. Інакше кажучи, криптосистема досконала, якщо її не можна зламати навіть за допомогою нескінченного числа операцій. Отже, незалежно від алгоритмічних досягнень і досконалості обчислювальної техніки абсолютно стійку схему зламати неможливо. У літературі можна натрапити й на інший термін, закріплений за абсолютною стійкістю, а саме: теоретико-інформаційна стійкість.

Шифр зсуву, шифр заміни, шифр Віженера являються обчислювально не захищені. До обчислювально стійких систем можна віднести криптографічні системи DES, RSA, Ель-Гамаля. Процес шифрування полягає в заміні кожної букви на іншу, віддалену від вихідної на певне число позицій в алфавіті залежно від значення ключа. Так, наприклад, якщо ключ дорівнює 3, то буква «а» вихідного тексту в шифровці зображується «D», замість букви «b» з’явиться «Е» і т.ін. Слово «hello» буде представлено шифровкою «KHOOR».

Щоб дати формальне визначення абсолютної стійкості, зафіксуємо такі позначення: {P} - множина можливих відкритих текстів, тобто простір повідомлень, {K} - сукупність можливих ключів; {C} - множина шифротекстів. Кожна множина є простором подій, в якому ймовірності позначаються як p(P = m), p(K = k), p(C = c). Будемо вважати, що будь-які події незалежні. Користувачі не міняють ключів шифру залежно від змісту відкритого тексту. Символом Ck)} позначимо множину всіх криптограм, які отримані з простору повідомлень шифруванням за допомогою ключа k:

 (4.3)

де Ек – шифруюча функція.

Має місце співвідношення:

 (4.4)

де Dк – розшифруюча функція.

Криптосистема, шифротекст в якій не дає жодної інформації щодо відповідного відкритого тексту, називається абсолютно стійкою, або досконалою. Має місце таке визначення: криптосистема є абсолютно стійкою, якщо рівність

** (4.5)

має місце для всіх відкритих текстів m є {Р} та всіх криптограм m є {С}.

Для абсолютно стійкої криптосистеми має місце нерівність

 (4.5)

де #{K} — число можливих ключів, #{С} — число можливих шифрограм, #{P} — розмір простору повідомлень.

Прикладом системи з абсолютною стійкістю є шифр Вернама.

Шифр Вернама. Головна операція описаного модифікованого шифру зсуву - додавання за модулем 26, що, з огляду на обчислювальну техніку, є дуже доро­гим, тоді як двійкова арифметика порівняно легка. У першу чергу нас цікавить додавання за модулем 2.

У 1917 р. Гільберт Вернам запатентував шифр, заснований на цій операції, який тепер називають шифром Вернама, або одноразовим шифр-блокнотом. Для пересилання рядка бітів необхідний ключ, що складається з тієї самої кількості двійкових знаків, що і повідомлення. Кожен біт рядка посилається, складається за модулем 2 з відповідним знаком ключа, і виходить криптограма.

Будь-який ключ дозволяється використовувати для шифрування тільки один раз, звідси і назва «одноразовий шифр-блокнот». Таким чином, розподіл ключів тут - основна проблема.

5. ТЕХНОЛОГІЇ ФІЛЬТРАЦІЇ КОНТЕНТУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

5.1 Узагальнена модель фільтрації контенту

Як відомо, базовою ідеологією концепції World Wide Web є надання серверним процесом того чи іншого ресурсу на запит клієнтського. З метою аналізу технологій фільтрації, які можуть використовуватись для обмеження доступу до небажаних інформаційних ресурсів, розглянемо процес одержання web-ресурсу на запит користувача (або програмного забезпечення) на різних етапах проходження запиту та відповіді (рис. 5.1). З метою спрощення відображення цього процесу будемо вважати, що під час запитів використовується лише протокол HTTP [8.23] (Hyper Text Transfer Proocol).

Як показано на рис. 5.1, ініціатором запиту на одержання інформаційного ре­сурсу може виступати як звичайний користувач, так і автоматизований засіб (ме­неджер завантажень, шкідливе програмне забезпечення тощо). Незалежно від джерела ініціативи для безпосередньої реалізації запиту використовується спеціалізований програмний засіб, який підтримує функціональність HTTP- клієнту - веб-клієнт. Найбільш розповсюдженою та відомою формою веб-клієнтів є веб-браузери. Однак з цією метою можуть використовуватись і будь-які програмні бібліотеки з підтримкою протоколу HTTP та можливістю встановлення TCP-з’єднання з будь-яким вузлом мережі, відправлення HTTP-запитів та одер­жання HTTP-відповідей.

Слід зазначити, що початковою точкою, в якій може здійснюватися фільтрація запитів на одержання web-ресурсів або фільтрація контенту запитаних ресурсів, може бути саме веб-клієнт. Більшість поширених веб-браузерів активно використовують цю можливість через блокування доступу до певних доменних імен, аналіз URL (Uniform Resource Locator) та/або завантаженого контенту на наявність заборонених слів (або частин слів). Слід, однак, зазначити, що важливим недоліком блокування доступу до інформаційних ресурсів за допомогою веб-браузера є можливість використання іншого веб-клієнта в обхід будь-якого обмеження.

Наступним можливим засобом для фільтрації запитів та одержаного контенту може бути міжмережний екран, установлений на робочій станції користувача. Незважаючи на дещо більшу надійність (забезпечується незалежність від використаного веб-клієнта), такий спосіб блокування також має низку вагомих недоліків. Так, наприклад, переважна більшість міжмережних екранів підтримують лише блокування за IP-адресою, що може призвести до помилкового блокування ресурсу, який розміщується на одному сервері (з тією самою IP-адресою) з небажаним контентом. Окремим недоліком блокування на міжмережному екрані робочої станції є різке збільшення навантаження на апаратну платформу при зростанні кількості записів у списках фільтрації. Це пояснюється тим, що при застосуванні міжмережних екранів фільтрації та обробці підлягає кожен IP-пакет, що проходить крізь екран.

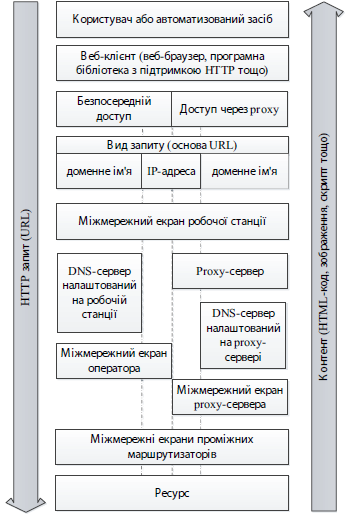


Рис. 5.1 Процес одержання web – ресурсу

Запит на одержання веб-ресурсу представлено у вигляді URL, основу якого становить доменне ім’я або IP-адреса (наприклад, 193.186.15.1). Якщо TCP-з’єднання встановлюються безпосередньо з вузлом, на якому розміщується необхідний ресурс, а основою запитуваного URL є доменне ім’я, наступним етапом проходження HTTP-запиту є визначення IP-адреси цього доменного імені. Визначення здійснюється шляхом надсилання запиту до DNS-сервера, налаштованого на робочій станції користувача. Слід зазначити, що DNS-сервер при цьому може також бути використаний для фільтрації HTTP-навантаження. Така фільтрація може бути забезпечена за рахунок того, що DNS-сервер може замість реальної IP-адреси запитаного ресурсу повернути робочій станції іншу адресу - в разі якщо запитане доменне ім’я підпадає під політику фільтрації. Певним недоліком такого способу блокування є легкість обходу системи обмеження доступу на робочій станції шляхом конфігурування іншого DNS-сервера або за рахунок внесення необхідних записів до локальних файлів доменних імен.

Залежно від налаштувань веб-клієнта (а в деяких випадках залежно від налаштування мережі доступу) TCP-з’єднання може встановлюватися з сервером-посередником (проксі-сервером). У цьому разі будь-який запит (на основі доменного імені або IP-адреси) оброблюється цим сервером. Така властивість proxy-серверів дозволяє створювати на їх основі надійні системи фільтрації. Певним недоліком таких систем фільтрації є неможливість фільтрації навантаження, відмінного від HTTP- навантаження (у цьому випадку, як правило, застосовується блокування інших видів навантаження на міжмережних екранах), а також необхідність застосування додаткових методів оптимізації обробки запитів при великій кількості робочих станцій, що працюють через один сервер. Слід також зазначити, що при використанні під час запиту URL на основі доменного імені proxy-сервер також здійснює звернення до DNS-сервера. Однак в цьому випадку proxy-сервер звертається до DNS- сервера, налаштованого адміністратором proxy-сервера. Така властивість може бути використана при створенні багатоступінчастих систем фільтрації контенту.

Дальший шлях проходження запиту до необхідного ресурсу може містити в собі низку міжмережних екранів, які розміщуються у провайдера (оператора) послуг доступу до мережі Інтернет з боку клієнта, який надсилає запит, з боку сервера, який надає необхідний ресурс або з боку сервера-посередника. Крім цього, міжмережні екрани можуть розміщуватись на будь-яких проміжних маршрутизаторах, через які здійснюється проходження запиту. Кожен з цих міжмережних екранів може використовуватися для організації системи фільтрації контенту і при цьому мати різну політику блокування та використовувати різні методи та підходи до фільтрації.

При надсиланні ресурсом відповіді на запит клієнта контент у зворотному порядку проходить ті самі кроки, що й запит (за винятком DNS-серверів). Якщо при проходженні запиту аналізу підлягає лише URL запитаного ресурсу, то в цьому випадку системи фільтрації можуть здійснювати безпосередньо аналіз самого контенту (наприклад, аналіз наявності в тексті сторінки тих чи інших слів). За результатами обробки контент може бути заблокований або замінений на інший (наприклад, замість зображення порнографічного характеру може бути відображено затемнений прямокутник такого самого розміру).

Як було показано вище, між клієнтом та сервером в мережі Інтернет можуть використовуватись різні засоби фільтрації, які реалізовано на рівні веб-клієнтів, proxy-серверів, DNS-серверів або міжмережних екранів.

На рис. 5.2 подано класифікаційну модель фільтрації веб-контенту в мережі Інтернет. Основу моделі становлять чотири розглянуті вище засоби фільтрації: веб-клієнт, proxy-сервер, DNS та міжмережний екран. Кожен з цих засобів являє собою окремий рівень фільтрації та може мати різну архітектуру, використовува­ти різні види та підходи до фільтрації, а також мати різні методи формування списків блокування. Розглянемо більш детально кожну зі складових пропонованої моделі.

З архітектурної точки зору, кожен з наведених на рис. 5.2 засобів фільтрації може бути побудованим за централізованою або децентралізованою схемою. Централізована схема передбачає фільтрацію навантаження на центральному вузлі в режимі «online». Для цього будь-який з наведених вище засобів фільтрації може переспрямувати все навантаження до центрального вузла для прийняття рішення про необхідність фільтрації.

Незважаючи на те, що така схема має надвисоку ефективність (миттєве оновлення списків блокування, легкість підтримки тощо), вона має низку досить істотних недоліків:

- обладнання обробки повинно мати відповідну потужність, щоб не вносити велику затримку та не створювати незручності користувачам;

- центральний вузол повинен мати велику пропускну здатність каналів;

- у разі виходу з ладу центрального вузла система зупиняється.

Децентралізована схема передбачає фільтрацію навантаження безпосередньо на місцях. Це можуть бути як кінцеві робочі станції користувачів (веб-браузер, міжмережний екран робочої станції тощо), так і вузлове мережне обладнання підприємств та організацій (DNS-сервер, proxy-сервер або мережний екран робочого маршрутизатора). Така схема дозволяє підвищити відмовостійкість, оскільки кожен вузол функціонує автономно, за рахунок ускладнення процесу обслуговування системи, однак заздалегідь передбачає збільшення витрат на її реалізацію.

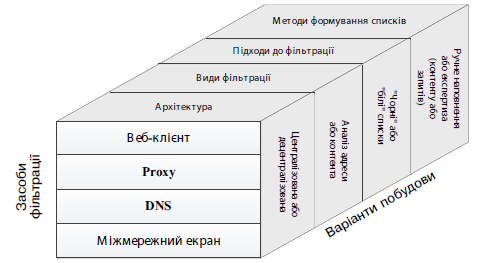


Рис. 5.2 Класифікаційна модель фільтрації web – контенту в мережі Інтернет

У будь-якій системі обмеження доступу можуть застосуватися такі види фільтрації, як фільтрація за адресою ресурсу та фільтрація за контентом (змістом ресурсу). Слід також зазначити, що певні системи можуть використовувати одно­часно обидва види фільтрації. Як видно з рис. 5.2, технологічно фільтрація за адресою ресурсу застосовується вже на етапі надсилання запиту користувачем або автоматизованою системою. а фільтрація за контентом застосовується при переда­ванні інформації від ресурсу до користувача. Основними перевагами фільтрації за адресою ресурсу є порівняно низька завантаженість вузла обмеження доступу (немає необхідності оброблювати великі масиви інформації). а також можливість фільтрації різномовних ресурсів. а також ресурсів. які практично не містять текстових частин (наприклад, використовуються лише інтерактивні засоби - flash, java тощо). У свою чергу, фільтрація за контентом часто дозволяє забезпечити значно більш надійний рівень фільтрації за рахунок виявлення на сторінці певних слів або частин слів, що внесені до списку фільтрації. Слід також зазначити, що фільтрація за контентом може мати дуже велику кількість ступенів складності (аналіз текстової частини сторінки, аналіз зображень тощо), що може значно збільшити час обробки сторінки системою фільтрації.

За своїми підходами до фільтрації контенту всі системи можна умовно поділити на два класи: «усе, що прямо не дозволено, те заборонено» («білі» списки) та «усе, що прямо не заборонено, те дозволено» («чорні» списки). Застосування того чи іншого підходу залежить від обраної в системі політики обмеження доступу. Так, наприклад, використання «білих» списків більш притаманне військовим організаціям, а також країнам із законодавчо закріпленою цензурою. У свою чергу, «чорні» списки широко використовуються в системах фільтрації, в навчальних закладах та науко­вих установах. Слід зазначити, що певні системи фільтрації (незалежно від засобу фільтрації) контенту підтримують обидва підходи до фільтрації та дозволяють користувачеві (або керівникові) самостійно обирати політику фільтрації.

Незалежно від використаного підходу до фільтрації різноманітні системи можуть використовувати різноманітні методи формування списків («білих» та/або «чорних»). Одним з найбільш поширених методів формування списків є їх ручне наповнення за рахунок звернень користувачів або особистого пошуку негативного контенту розробниками системи обмеження доступу. Очевидним недоліком такого методу є велика тривалість формування списків та низька швидкість реагування на появу нових негативних ресурсів. Альтернативним до ручного наповнення є експертне (у тому числі на основі автоматизованих систем експертного оцінювання) формування списків на основі аналізу контенту, що було переглянуто користувачами системи обмеження доступу.

Механізми, які використовує той чи інший засіб для блокування (наприклад, спосіб оновлення та застосування списків блокування), залежать від програмної реалізації веб-клієнта, міжмережного екрана, DNS або proxy-сервера. При цьому три останні засоби можуть використовуватися декілька разів у різній послідовності, утворюючи цілий ланцюг систем обмеження доступу, кожна ланка якого може використовувати різні види та підходи до фільтрації, а також різні методи формування списків блокування та бути побудованою за централізованою або децентралізованою схемою.

Яскравими прикладами побудови системи фільтрації на основі веб-браузера можуть бути система фільтрації браузера Microsoft Internet Explorer (ICRA) [24], а також система фільтрації, основана на використанні веб-браузера Buddy Browser [25]. При цьому якщо система фільтрації Microsoft Internet Explorer працює за децентралізованою схемою, то Buddy Browser пропускає навантаження користувачів через власну систему фільтрації.

Як приклад побудови систем фільтрації на основі proxy-серверів можна навести Всеукраїнську систему обмеження доступу до нецільових ресурсів мережі Інтернет [26]. В основу системи покладено принцип установлення в кожній організації власного proxy-сервера, який має базу даних заборонених ресурсів (децентралізована схема). Систематичне оновлення бази організоване за рахунок централізованої експертної обробки службових журналів зазначених серверів на базі інформаційного центру з дальшим періодичним формуванням оновленої редакції бази даних заборонених ресурсів та її розсиланням (в автоматичному режимі) до всіх proxy-серверів.

Типовим представником систем фільтрації на основі DNS-серверів є система OpenDNS [27]. Систему побудовано за централізованою схемою з використанням лише аналізу адреси для прийняття рішення про необхідність фільтрації, а також на основі використання «чорних» списків.

Таке розмаїття технологій породжує велику кількість варіантів побудови систем фільтрації, кожен з яких може вважатися оптимальним для тих чи інших умов. Крім технологічних аспектів, у разі вибору тієї чи іншої системи користувачі часто спираються і на інші критерії: вартість і складність упровадження та підтримки, сумісність системи фільтрації з іншими мережними сервісами.

5.2 Спільна робота сучасних засобів фільтрації контенту

Зважаючи на бурхливий розвиток мережі Інтернет, який спостерігається останніми роками, дедалі більшої актуальності набуває питання фільтрації контенту під час його передавання від інформаційного ресурсу до споживача. Небхідність розв’язання таких завдань, як захист дітей в мережі Інтернет, блокування небажаної реклами та шкідливого програмного забезпечення, дотримання корпоративної політики щодо заборони доступу до розважальних ресурсів у робо чий час та навіть цензура (для країн із законодавчо обмеженою свободою слова) створили передумови розвитку всієї індустрії систем фільтрації контенту (СФК). Результатом цього розвитку стала поява великої кількості програмних та програмно-апаратних рішень, призначених для блокування доступу до інформаційних ресурсів мережі Інтернет на різних рівнях (безпосередньо на робочій станції користувача, на стороні провайдера, в точках обміну навантаженням операторів телекомунікацій тощо).

Навіть поверхневий аналіз різних засобів фільтрації (веб-клієнт, proxy-сервер, DNS-сервер, міжмережний екран) показує наявність переваг і недоліків та доз­воляє зробити висновок про доцільність комбінування різних варіантів та підходів з метою створення комплексних СФК.

Під комплексною системою фільтрації контенту (КСФК) будемо розуміти систему, що складається з двох чи більше засобів фільтрації, кожен з яких може вико­ристовувати різні види, методи та підходи до фільтрації контенту. В межах КСФК засоби можуть працювати у послідовному (підсилюючи один одного) або в паралельному (доповнюючи один одного) режимі. У послідовному режимі адреса або контент, що пройшли процедуру фільтрації на одному із засобів, потрапляють на вхід іншого засобу з метою повторної обробки (наприклад, за допомогою інших методів). У свою чергу, паралельний режим припускає фільтрацію адреси через використання одного засобу фільтрації, а фільтрацію контенту із використанням іншого.

З метою спрощення розуміння наступного матеріалу запровадимо умовні позначення для систем фільтрації контенту із врахуванням класифікаційної моделі, запропонованої в попередньому підрозділі. Загальну структуру умовного позначення наведено на рис. 5.3.

Відповідні елементи позначення (рис. 5.3) можуть мати такі значення (відповідно до порядку слідування):

засоби фільтрації: міжмережний екран — «F» (firewall), DNS-сервер — «D», proxy-сервер - «Р» (proxy), веб-клієнт (або інше прикладне програмне забезпечення) - «В» (browser);

архітектура: централізована - «С» (centralized) та децентралізована — «D» (decentralized);

види фільтрації: за контентом - «С» (content), за адресою — «A» (address);

підходи до фільтрації: «чорні» списки — «В» (black), «білі» списки «W» (white);

методи формування списків - вручну – «М», експертами – «Е», автоматично – «А»

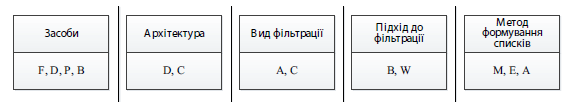


Рис. 5.3 Умовні позначення систем фільтрації контенту

Таким чином, система, що базується на використанні ргоху-серверів, як засобів фільтрації, передбачає децентралізовану архітектуру, фільтрацію лише за адресою на основі «чорних» списків при ручному методі їх формування може бути позначено, як е|б|л|в|м

У разі коли СФК має дві чи більше властивостей одночасно (наприклад, підтримує фільтрацію як за «білими», так і за «чорними» списками), відповідний розділ позначається обома літерами одночасно (наприклад, «BW»). У свою чергу, комплексні СФК (на відміну від звичайних) можуть мати дві чи більше літери в секції «Засоби» (наприклад, «DB» у разі одночасного комбінування фільтрації на DNS-сервері та на веб-клієнті) за умов, якщо інші властивості в системі фільтрації однакові, або можуть позначатися як серія записів про звичайні СФК. Як було зазначено раніше, кожен із розглянутих засобів фільтрації має низку недоліків, які можуть бути цілком або частково усунені за рахунок комбінування з іншими засобами.

Одним із найбільш істотних недоліків фільтрації на міжмережному екрані є стрімке зростання навантаження на обладнання при збільшенні кількості записів у списках фільтрації. Це пояснюється тим, що аналіз при цьому здійснюється для кожного пакета, а не для запитів на створення сесії. Очевидно, що, використовуючи міжмережний екран лише для спрямування навантаження на DNS або proxy- сервер, зазначений недолік може бути подоланий, однак при цьому роль самого міжмережного екрана, як засобу фільтрації контенту, набагато зменшується. У свою чергу, використовуючи як основний засіб фільтрації вебклієнт, при цьому обмежуючи використання інших засобів, безпосередньо на міжмережному екрані можна перекласти завдання фільтрації безпосередньо на вбудовані до веб-клієнта механізми та досить надійно обмежити використання інших видів навантаження.

Іншим важливим недоліком міжмережного екрана, як засобу фільтрації, є обмеженість діалогу з користувачем при блокуванні того чи іншого ресурсу. Це пояснюється тим, що прикладний процес (у разі, коли міжмережний екран працює на іншому вузлі) не може відрізнити блокування пакета на міжмережному екрані від його втрати під час передавання через мережу. вирішити цю проблему можна, лише комбінуючи міжмережний екран із іншими засобами фільтрації з метою делегування їм функцій фільтрації.

Останній з найвідоміших недоліків міжмережного екрана (з точки зору фільтрації контенту) - висока імовірність помилкового обмеження та неефективність фільтрації за контентом - пояснюється тим, що під час фільтрації за контентом міжмережний екран має не тільки обробляти кожен пакет окремо, а й не має можливості проводити аналіз усього інформаційного блоку. Так, наприклад, завдяки фрагментації блоку даних на пакети перша частина ключової фрази, яка підпадає під шаблони фільтрації, може перебувати в одному пакеті, а друга частина - в іншому. У такому разі обидва пакети подолають обмеження. Вирішенням проблеми, як і в попередніх випадках, може стати доповнення міжмережного екрана фільтрацією на proxy-сервері або безпосередньо на вебклієнті. Винятком є лише використання DNS-сервера, який не може бути використаний для фільтрації контенту взагалі.

Таким чином, комбінації «FP» та «FB» дозволяють подолати основні недоліки міжмережного екрана як засобу фільтрації, однак при цьому фактично відбудеться заміщення одного засобу на інший. При цьому комбінація «FD» дозволяє усунути лише частину недоліків та не може розглядатися як ефективний засіб у разі потреби забезпечення фільтрації за контентом.

Одним із істотних недоліків фільтрації з використанням DNS-сервера є можливість обходу системи шляхом конфігурування іншого DNS-сервера або внесенням запису до hosts-файлу. Цілком вирішити цю проблему можна лише за рахунок надіслання всіх запитів до proxy-сервера. У свою чергу, використання міжме режного екрана або веб-клієнта дозволяє вирішити проблему частково (наприклад, блокування звернення до інших DNS-серверів) або взагалі не позбавляє СФК зазначеного недоліку.

Другим відомим недоліком систем фільтрації на DNS-серверах є неможливість фільтрації за контентом. З огляду на наведені вище пояснення щодо обробки контенту міжмережним екраном вирішити цю проблему шляхом комбінування саме цим способом неможливо. Однак надсилання запитів через proxy-сервер або із власного веб-клієнта дозволяє повною мірою забезпечити фільтрацію контенту. Таким чином, цілком вирішити означені проблеми фільтрації контенту на DNS- серверах можна лише за рахунок комбінування з proxy-сервером, який використовується для фільтрації контенту та фільтрації запитів, що містять IP-адреси.

Одним з основних недоліків засобів фільтрації на основі proxy-серверів є неможливість або складність обмеження навантаження, що передається за допомогою відмінних від HTTP протоколів. Очевидно, що частково цю проблему можна вирішити за допомогою міжмережних екранів (наприклад, за рахунок блокування інших видів навантаження). Однак враховуючи великий обсяг споживання обчислювальних ресурсів, більш прийнятною буде організація додаткової фільтрації з використанням DNS-серверів. Іншим недоліком proxy-серверів (як засобів фільтрації) є великий час обробки запитів при збільшенні кількості записів у списках фільтрації. Це пояснюється тим, що порівняно, наприклад, із DNS-сервером на proxy-сервери покладено низку різноманітних функцій (кешування, передавання контенту тощо). Вирішенням цієї проблеми може бути розділення функцій фільтрації між proxy- та DNS-серверами.

Найбільш вагомим недоліком фільтрації на веб-клієнті є складність адміністрування та підтримки при зростанні кількості вузлів. Очевидно, що підтримувати та стежити за цілісністю великої кількості копій програмного забезпечення веб- клієнта набагато складніше, ніж за системами фільтрації, розміщеними на одному сервері. Як і в попередніх випадках, вирішенням проблеми може бути делегування функцій фільтрації proxy- або DNS-сервера.

# **6. ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА БЕЗПЕКИ В НАДЗВИЧАЙНИХ СИТУАЦІЯХ**

У відповідності з законом України «Про охорону праці» жодне виробництво, підприємство, цех, робочий ділянку не можуть бути введені в експлуатацію, якщо на них не будуть забезпечені здорові та безпечні умови праці.

В лабораторії з ПК встановлено наступне обладнання:

- обчислювальна техніка (ЕОМ потужністю 350 Вт);

- монітори.

Функціональна схема обладнання, яке використовується у роботі, зображена на рис.6.1.

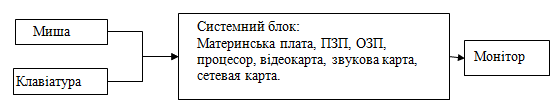


Рис. 6.1– Функціональна схема обладнання

Дане обладнання призначене для роботи операторів ЕОМ зі створення систем автоматизованого управління виробництвом, різного програмного забезпечення, проектно-конструкторських робіт і отримання кінцевих результатів робіт у вигляді документів: лістинги програм, схеми, креслення та ін.

# **6.1 Промислова безпека в проектному відділі**

За ступенем небезпеки ураження електричним струмом за НПАОП 40.1-1.21-98 дане приміщення відноситься до класу приміщень без підвищеної небезпеки, так як вологість 40-60% і виключена можливість одночасного дотику людини до корпусів електрообладнання і заземленим металевим конструкціям будівель і споруд, які мають зв'язок із землею.

Електропостачання відділу здійснюється від 3-х фазної мережі з глухозаземленою нейтраллю, змінний струм, напруга 380/220 В. відповідно до вимог НПАОП 40.1-1.32-01.

Передбачені наступні міри електробезпеки:

- конструктивні міри електробезпеки;

- схемно-конструктивні міри електробезпеки;

- експлуатаційні міри електробезпеки.

Конструктивні міри електробезпеки забезпечують таке конструктивне рішення, яке запобігає можливість дотику людини до струмопровідних частин приладів і обладнання.

Для усунення можливості поразки електричним струмом при дотику працівника до струмопровідних металевих частин, усі рубильники встановлюються в закритих корпусах, з'єднувальні кабелі та шини електроживлення підведені до задньої панелі апаратури і недоступні людині. Застосовується блоковий монтаж.

Згідно з вимогами НПАОП 40.1-1.32-01 для електроустановок змінного струму напругою до 1000В і глухозаземленою нейтраллю застосовується занулення. У приміщенні лабораторії з ПК використана система занулення TN-S.

Комплекс необхідних заходів по техніці безпеки визначається виходячи з виду електроустановки та її номінальної напруги, умов середовища, типу приміщення і доступності електрообладнання.

Яке експлуатується обладнання не є джерелом механічних, або радіаційних небезпек, але є споживачем електричної енергії.

В приміщенні лабораторії, не частіше одного разу на рік, виконується контроль ізоляції. Перш за все,від мережі відключаються всі споживачі, включаючи ДБЖ, подовжувачі та трійники. Потім на щитку відключаються автомати», відповідні досліджуваним групам і з допомогою мегаомметра проводу вимірюються попарно: фаза-фаза, фаза-нуль, нуль, земля. У разі виявлення занадто низького опору необхідно провести додаткові роботи: встановити ділянку ланцюга, на якому порушена ізоляція і негайно усунути дефект.

З працівниками проводиться вступний, первинний, повторний, цільовий, а при необхідності і позаплановий інструктаж. Зміст всіх інструктажів відповідає вимогам НПАОП 0.00-4.12-05.

# **6.2 Забезпечення виробничої санітарії та гігієни праці**

Роботи в даному приміщенні проводяться сидячи і не потребують систематичного фізичної напруги. Згідно ДСН 3.3.6-042-99 робота відноситься до категорії легкої Іа (енерговитрати до 120 ккал/ч). Робочі місця характеризуються наступними мікрокліматичними умовами:

а) відносна вологість повітря 40 - 60%;

б) температура:

- у холодний період: оптимальна 22-24 С, допустима верхня - 25 С, нижня - 21 С;

- в теплий період: оптимальна 23-25 С, допустима верхня - 28С, нижня - 22 С;

в) швидкість руху повітря:

- оптимальна - 0,1 м/с, допустима - 0,1м/с.

Підтримання на даному рівні параметрів, що визначають мікроклімат, здійснюється за допомогою кондиціонування в теплу пору року і при виділенні великої кількості тепла від обладнання з використанням опалення в холодну.

Шумове забруднення у відділі становить 50дБ, що не перевищує норму.

Приміщення з ЕОМ має природне та штучне освітлення відповідно до ДБН Ст. 25-28-2006 «Природне і штучне освітлення». Природне світло проникає через бічні светопроеми, зорієнтовані на північний схід, і забезпечувати коефіцієнт природної освітленості (КЕО) не нижче 1,5%.

Для забезпечення нормованих значень освітлення в приміщеннях з ВДТ ЕОМ загального та персонального користування очищають віконне скло та світильники не рідше ніж 2 рази на рік та своєчасно проводять заміну перегорілих ламп.

Так як домінуючим шкідливим фактором є підвищена температура повітря робочої зони, необхідно розробити систему кондиціювання повітря в приміщенні.

Для дотримання вимог техніки протипожежної безпеки та ергономіки в приміщенні встановлюються сучасні робочі столи та рідкокристалічні екрани. Працівнику для профілактики порушень і підтримки високої працездатності пропонується дотримуватися регламентовані перерви для відпочинку. Рекомендується в період роботи робити дві перерви по 15 хвилин, перший до обідньої перерви, другий – після. Головними елементами робочого місця є письмовий стіл і крісло. Основним робочим положенням є положення сидячи. Робоче місце для виконання робіт у положенні сидячи організується відповідно до ДСТУ 12.2.032-78. При роботі в положенні сидячи рекомендуються такі параметри робочого простору: довжина столу – 1000 мм, ширина – 800 мм, висота – 730 мм. Для задоволення вимог фізіології, конструкція робочого сидіння задовольняє наступним основним вимогам:допускає можливість зміни положення тіла, допускає регулювання висоти в залежності від росту працюючої людини, має злегка увігнуту поверхню, має невеликий нахил назад.

# **6.3 Безпека в надзвичайних ситуаціях в лабораторії з ПК**

Даний пункт розглядається відповідно до закону України «Про цивільного захисту».

У регіоні найбільш імовірними надзвичайними ситуаціями (НС), є надзвичайні ситуації техногенного характеру – це транспортні аварії (катастрофи), пожежі, неспровоковані вибухи, аварії з викидом небезпечних хімічних речовин, раптове руйнування споруд та будівель. Для лабораторії з ПК найбільш вірогідним НС є пожежа.

Пожежі в приміщеннях з ЕОМ представляють особливу небезпеку, оскільки зв'язані з великими матеріальними втратами.

Категорія приміщення по пожежній вибухонебезпечності згідно ДБН Ст. 1.1.7-2002 має І ступінь вогнестійкості, а за пожаровзрывоопасности відноситься до категорії В.

Дане приміщення відноситься до зони класу П-ІІа по ПУЕ-2011, так як це виробниче приміщення, є меблі з дерева і ДВП. Можливі причини виникнення пожежі у приміщенні роботи операторів ЕОМ:

- недотримання правил експлуатації електронно-обчислювальної техніки;

- недотримання правил пожежної безпеки;

- перегрів струмоведучих частин обладнання в слідстві освіти високого перехідного опору в місцях з'єднань;

- несправність загального чи місцевого освітлення робочих місць.

Згідно з вимогами протипожежної безпеки в приміщенні встановлюється 2 вуглекислотних вогнегасника ВВК-1.4 (з розрахунку 1 на 20 м2), які застосовуються при гасінні невеликих вогнищ і можуть бути використані для гасіння електроустановок, що знаходяться під напругою. У відповідності з ГОСТ 12.4.026-76 ці кошти пофарбовані в яскраво-червоний колір і перебувають у легкодоступному місці, при виході з приміщення.

Приміщення лабораторії обладнано системою автоматичної пожежної сигналізації з застосуванням теплових датчиків типу ПОСТ-1 3 штуки, (з розрахунку 2 датчика на кожні 20 м2 площі), налаштованих на температуру спрацьовування 70°С.

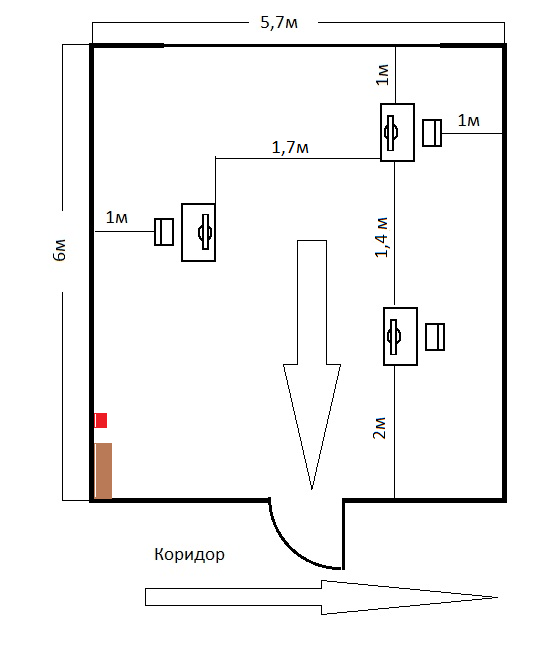
Організаційні заходи пожежної профілактики:

- навчання персоналу правилам пожежної безпеки;

- видання необхідної інструкцій і плакатів, плану евакуації   
персоналу у разі пожежі;

- виготовлення і застосування засобів наочної агітації по забезпеченню пожежної безпеки.

План евакуації показаний на рис.6.2:



- путь евакуації

 - ящик з піском - вогнегасник

Рис. 6.2 – Схема евакуації при пожежі

Протидія пожежам здійснюється в процесі забезпечення пожежної безпеки. Для цього встановлюються вимоги пожежної безпеки і протипожежні режими, здійснюються заходи пожежної безпеки.

У разі виникнення пожежі необхідно організувати заходи по евакуації людей з будівлі, наявними для цього всіма силами і засобами. Перевірити справність і включення в роботу автоматичних систем протипожежного захисту.

ВИСНОВКИ

У процесі роботи над дипломним проектом було проведене дослідження безпеки сучасних телекомунікаційних мереж.

Була виконана систематизація та порівняльний аналіз методів, що забезпечують безпеку сучасних телекомунікаційних мереж.

У процесі роботи були проведені систематизація і вивчення основних понять що пов`язані з сучасними телекомунікаціями. Проведено аналіз проблем інформаційної безпеки. Проведено вивчення понять технічного захисту інформації, видів та методів захисту , виконано спеціальний розділ дипломного проекту.

Враховуючи стрімкий розвиток телекомунікацій них мереж майже в усіх галузях виробництва та бізнесу, можна зробити висновок про сто відсотково виправдану необхідність вкладати як фінанси, так і інтелектуальні ресурси в розвиток такого роду зв`язку, взагалі, та розвиток і удосконалення методів, що забезпечують безпеку інформаційного контенту для користувачів, зокрема.

У розділі «Заходи з охорони праці» виконаний аналіз потенційних небезпек, розроблені заходи з техніки безпеки, заходи, що забезпечують виробничу санітарію та гігієну праці, та охорони навколишнього середовища.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗИ 1.1-003-99. Терминология в отрасли защиты информации в компьютерных системах от несанкционированного доступа [Электронный ресурс] / Утв. приказом ДСТСЗИ СБУ от 28.04.1999 № 22. - К.: ДСТСЗИ СБУ, 1999. - 30 с.
2. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.Г. Ивашко. - Г.: Горячая линия - Телеком, 2000. - 452 с.
3. Рекомендация МСЭ-T Е.408. Требования к безопасности сетей электросвязи [Элек­тронный ресурс]. - Женева, 2004. - 21 с. Recommendation ITU-T X.800. Security architec­ture for Open Systems Interconnection for CCITT applications [Электронный ресурс]. - Geneva, 1991. - 48 с. - Режим доступа: <http://www.itu.int/net/home/index.aspx>
4. Кононович В.Г. Технічна експлуатація систем захисту інформації теле­комунікаційних мереж загального користування. Частина 3. Архітектура безпеки: Кон­цепція захисту інформації: [навч. посібник для вузів, затверджений Міністерством транс­порту та зв’язку України] / Кононович В.Г. - ОНАЗ. - Одеса, 2009. - 194 с.
5. Рекомендация МСЗ-T Е.408. Требования к безопасности сетей электросвязи [Элек­тронный ресурс]. - Женева, 2004. - 21 с. - Режим доступа: <http://www.itu.int/net/home/> index.aspe.
6. Стандарт ISO/IEC 15408:2000. Information technology - Security techniques - Evaluation criteria for IT security. - Part 1: Introduction and general model. - Part 2: Security functional requirements. - Part 3: Security assurance requirements.
7. Перспективы применения международного стандарта ISO/IEC в Украине / Г. Бон­даренко, Л. Скрыпник, И. Горбенко, А. Потий - Журн.: «Правовое, нормативное и метро­логическое обеспечение системи защиты информации в Украине», вып. 3-й. - Киев. - 2001. - С. 7-26.
8. Леваков А. Анатомия информационной безопасности США [Электрнонный ресурс] - Jet Info online № 6 (109), 2002. - 74 с. - Режим доступа: [http://daily.sec.ru/dailyp- blshow.cfn?rid=9&pid=5503&pos=13&stp=10](http://daily.sec.ru/dailyp-blshow.cfn?rid=9&pid=5503&pos=13&stp=10).
9. Рекомендация МСЭ-T ^.1205. Безопасность электросвязи. Обзор кибербезопаснос­ти. - Женева, 2009. - 55 с.
10. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України в редакції від 31.05.2005 р. № 2594-ІУ / Відомості Верховної Ради України. - № 26, ст. 347. - К.: 2007. - 13 с.
11. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. - [Чинний від 01.01.1998-12-19]. - К.: Держстандарт України, 1998. - 15 с.
12. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО «Изд. Машиностроение», 2009 - 508 с.
13. Про основи національної безпеки України [Електронний ресурс]: Закон України від 19.06.2003 р. № 964-ІУ, зі змінами від 15.12.2005 р. / Відомості Верховної Ради Ук­раїни. - № 14, ст. 116. - К.: 2006. - 16 с. - Режим доступу: [http://www.dstszi.gov.ua/dst- szi/con-](http://www.dstszi.gov.ua/dst-szi/con-) trol/uk/publish/article?art\_id=43411& cat\_id=38828.
14. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В.Ро- манец, П.А. Тимофеев, В.Ф. Шаньгин. Под ред. В.Ф. Шаньгина. - М.: Радио и связь, 1999. - 328 с.
15. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. - М.: ДМК Пресс, 2008. - 544 с.
16. Смарт Н. Криптографія / Н. Смарт. - М.: Техносфера, 2005. - 528 с.
17. International Telecommunication Union [Електронний ресурс]. - Режим доступу: [www.itu.int](http://www.itu.int).
18. Project Cleanfeed, [Електроний ресурс]. - Режим доступу: <http://en.wikipedia.org/> wiki/Cleanfeed\_(content\_blocking\_system).
19. Usage de l’internet dans le cadre pedagogique et protection des mineurs (CIRCU­LAIRE N2004-035 DU 18-2-2004). [Електронний ресурс]. - Режим доступу: [http://www.edu- cation.gouv.fr/bo/2004/9/MENT0400337C.htm](http://www.edu-cation.gouv.fr/bo/2004/9/MENT0400337C.htm)
20. Study Finds 25 Countries Block Web Sites, [Електронний ресурс]. - Режим доступу: <http://www.smh.com.au/>
21. Law no. 38.529, Asamblea Nacional de la Republica Bolivariana de Venezeula, «Ley de Proteccin de Nios, Nias y Adolescentes en salas de uso de Internet, Video Juegos y otros Multimedia», November 5, 2006.
22. Таненбаум Э. Компьютерные сети. 4-е изд. / Таненбаум Э. - СПб.: Питер, 2005. - 992 с.
23. Hypertext Transfer Protocol / [R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee] - HTTP/1.1. [Електронний ресурс]. - Режим доступу: <http://www.w3.org/Protocols/rfc2616/rfc2616.html>.
24. ICRA filtering using Microsoft Internet Explorer. [Електронний ресурс]. - Режим доступу: <http://www.icra.org/support/contentadvisor/setupv03/>.
25. Boddy Browser. [Електронний ресурс]. - Режим доступу: [http://www.buddybrows- er.com/Free-Parental-Controls.cfm](http://www.buddybrows-er.com/Free-Parental-Controls.cfm).
26. Єдина система обмеження доступу до нецільових ресурсів мєрєжі Інтернет в освітніх закладах України / [П.П. Воробієнко, В.А. Каптур, В.А. Коляденко, В.О. Са- модід]. - Журн.: Комп’ютер у школі та сім’ї. - 2009.- № 8.

27 Project OpenDNS. [Electronic resource]. - Access mode: <http://www.opendns.com/> solutions/overview/.