Міністерство транспорту та зв'язку України
Державна адміністрація зв'язку
_____
Одеська національна академія зв'язку ім. О.С. Попова
_____
Кафедра інформаційної безпеки та передавання даних

В. Г. Кононович, С.В. Стайкуца, Т. М. Тардаскіна, Т. М. Шинкарчук

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦИФРОВИХ ПРОГРАМНО КЕРОВАНИХ АТС

Навчальний посібник для курсового та дипломного проектування

Для студентів вищих навчальних закладів, які навчаються за напрямом «Системи захисту інформаційних та інформаційно-комунікаційних систем»

За редакцією члена-кореспондента МАЗ, кандидата технічних наук, доцента В.Г. Кононовича

Одеса 2011

УДК 004.056.5(075.8); 681.336; 342.4

Забезпечення інформаційної безпеки цифрових програмно керованих АТС Інформаційна безпека телефонного зв'язку: навч. посібник / [**Кононович В.Г., Стайкуца С.В., Тардаскіна Т.М., Шинкарчук Т.М.**] За ред. чл.-кор. МАЗ **В.Г. Кононовича**. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 168.

Представлені основні положення, поняття й визначення з проектування систем технічного захисту інформації програмно-керованих автоматичних телефонних станцій органів місцевої державної влади, їх організаційного, правового, технічного, методичного та програмно-апаратного забезпечення на етапах створення, вводу в дію та технічної експлуатації. Викладаються методи визначення витрат на інформаційну безпеку.

Висвітлено методологію проектування захисту автоматизованих центрів обробки викликів та надавання державних послуг на прикладі центру обробки викликів для органів внутрішніх справ.

Навчальний посібник буде корисний студентам бакалаврату, магістрату та слухачам курсів підвищення кваліфікації у сфері інформаційної безпеки.

Для студентів старших курсів вищих навчальних закладів.

СХВАЛЕНО
на засіданні кафедри інформаційної
безпеки та передавання даних
і рекомендовано до друку
Протокол № 5 від 07.04.2009 р.

ISBN

ВСТУП

Інформатизація, інтеграція, глобалізація та прискорений розвиток телекомунікацій справляють глибокий вплив як на життя людей, функціонування суспільства, держави, так і на органи державної влади. Складність розвитку технологій, виробничих та суспільних відносин спонукає органи державної влади до інформаційно-аналітичної діяльності, направленої на забезпечення прийняття ефективних рішень на основі оперування всеосяжною, повністю вірогідною, об'єктивною інформацією щодо становища справ, тенденцій, масштабів та очікуваних наслідків розвитку процесів життєдіяльності людей, спільнот, держави та світу на ближню та дальню перспективу.

Можливості неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів та інших загроз, викликають необхідність у забезпеченні інформаційної безпеки, яка є головною частиною економічної безпеки держави та національної безпеки в цілому.

Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності телекомунікаційних мереж.

Актуальним на сьогодні є підготовка фахівців, які вміють ефективно організувати захист інформації і володіють сучасними технологіями захисту інформації та мають достатню кваліфікацію для проектування та створення комплексних систем інформаційної безпеки.

Забезпечення інформаційної безпеки телекомунікаційних підрозділів державних підприємств та організація є допоміжною діяльністю в них і включає у себе реалізацію та підтримку трьох процесів: процесу проектування комплексної системи інформаційної безпеки, процесу створення, функціонування та вдосконалення системи інформаційної безпеки та процесу управління інформаційної безпеки.

Цей навчальний посібник повинен допомогти студентам, які навчаються за напрямом підготовки 1601 «Інформаційна безпека» оволодіти теоретичними знаннями та практичними навичками забезпечення інформаційної безпеки підприємства та звернути увагу на проблеми, які виникають в процесі створення комплексної системи захисту інформаційної безпеки на підприємствах зв'язку.

Наприкінці кожної частини наведено контрольні завдання та завдання до самостійної роботи, за допомогою яких можна перевірити рівень засвоєння теоретичного матеріалу.

Навчальний посібник підготували: к.т.н., доцент кафедри інформаційної безпеки та передавання даних В.Г. Кононович (вступ, розд. 2, 4, 5,), к.ф.н., доцент кафедри інформаційної безпеки та передавання даних С.В. Стайкуца (розд. 2, 4, 5), к.е.н., доцент кафедри менеджменту та маркетингу Т.М. Тардаскіна (вступ, 1,2,5), викладач кафедри інформаційної безпеки та передавання даних Т.М. Шинкарчук (розд. 3,6).

1 ПОСТАНОВКА ЗАДАЧІ ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕФОННИХ СИСТЕМ ЗАГАЛЬНОГО КОРИСТУВАННЯ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ

1.1 Роль та місце інформаційної безпеки в інформаційному суспільстві

Інформаційна безпека є однією з важливих складових глобальної безпеки. У процесі глобалізації, в умовах побудови інформаційного суспільства роль інформаційної безпеки посилюється і, навпаки, глобальні процеси впливають на інформаційну безпеку та взаємозв'язану з нею економічну, національну та глобальну.

Глобальний процес інформатизації суспільства, який є відображенням загальних закономірностей генезису цивілізації, сьогодні охопив усі сфери соціокультурної діяльності людини. Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій обумовлює кардинальні зміни в управлінні господарськими системами різних рівнів.

Особливості необмеженого та неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів та інших загроз, викликають необхідність у забезпеченні інформаційної безпеки, яка є головною частиною економічної безпеки держави та національної безпеки в цілому.

Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності інформаційно-телекомунікаційних мереж.

Завдяки стрімкому технологічному прогресу постає ряд життєво важливих питань щодо організації процесів оброблення, зберігання, поширення та захисту інформації в глобальних інформаційно-комунікаційних системах. Бо саме інформаційні технології та розвинена інфраструктура телекомунікацій відіграють сьогодні вирішальну роль у забезпеченні зростання продуктивності виробництва, адміністративного і господарського управління, у розширенні інформаційної взаємодії між людьми, у поширенні масової інформації, у процесі інтелектуалізації суспільства. Інформаційна безпека має важливе значення для того, щоб інформаційні технології могли відповідати очікуванням ділового світу, споживачів і урядів та щоб дійсно надавали всі ті потенційні вигоди, що їх забезпечують інформаційно-комунікаційні технології.

Інформаційна безпека в глобальних процесах набуває особливого значення і, внаслідок її тісних взаємовпливів з економічною та національною безпекою, вносить свій значний вклад у глобальну безпеку. Глобальною безпекою назвемо такий стан глобальних процесів та форм їхньої реалізації за якого забезпечуються:

– гармонічне поєднання інтересів народів, націй, держав та інтересів усього людства;

– ефективне вирішення завдань, які стоять перед людством та окремими державними, регіональними та місцевими адміністраціями;

– усебічний розвиток і забезпечення потреб кожної людини.

Глобальна безпека має фундаментальний характер і може бути досягнута за необхідного забезпечення її складових частин. Складовими частинами глобальної безпеки є: національна, економічна, інформаційна, технічна, юридична, фізична, соціальна, військова, екологічна, ресурсна, продовольча, енергетична, фінансово-грошова, цінова, демографічна, пожежна, медична, психологічна, психічна, кримінальна безпеки.

Особливості розвитку інформації, можливості необмеженого та неконтрольованого впливу, несанкціонований доступ, комп'ютерні віруси та інше гостро поставили перед суспільством проблеми інформаційної безпеки. Інформаційна безпека повинна здійснюватися комплексно та систематично з використанням повного набору засобів (організаційних, технічних, апаратно-програмних та ін.) щоб запобігти інформаційному тиску та в цілому будь-якій іншій небезпеці.

Зрозуміло, що становлення суспільства нового типу дуже гостро ставить питання інформаційної безпеки простору держави, людини, суспільства, а також створення ефективної системи забезпечення прав громадян і соціальних інститутів на вільне одержання, поширення і використання інформації. Це питання неможливо обійти, тим більше, що воно стає дуже актуальним зараз і для нашої країни.

Інформаційна безпека є більш вузьким поняттям і розглядається як складова національної безпеки. Інформаційна безпека містить у собі захист інформаційних мереж, ресурсів, програмних засобів, об'єктів інтелектуальної власності й інших нематеріальних активів, включаючи майнові інтереси учасників підприємницької діяльності [1].

В умовах глобалізації посилюється значимість проблем, які пов'язані з інформаційно безпекою, таких як:

– виникнення та зростання кіберзлочинності та кібертероризму;

– виникнення окремих видів інформаційної зброї та ведення глобальних інформаційних війн;

– втрата національної культури або злиття її з іншими, вплив культур країн світу та менталітету інших націй;

– стимулювання інформаційно-розвиненими державами „відпливу інтелекту" та капіталів;

– виникнення явищ „інформаційного вибуху", „інформаційного голоду" та „інформаційних війн".

– ускладнення вирішення питань збереження державної, комерційної, службової та персональної таємниці, тому що низький рівень вітчизняних інформаційних технологій обумовив побудову інформаційної інфраструктури України на базі імпортної техніки й технології;

– розвиток телебіометрики й сенсорних мереж у взаємодії людей між собою та навколишнім середовищем.

Інформаційна безпека не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації, вирішення цієї проблеми як складової національної безпеки. Тенденції розвитку сучасного світу характеризуються створенням єдиного глобального інформаційного простору

на планеті, отож, проблема інформаційної безпеки стає проблемою колективною, а не окремо взятої країни.

1.2 Сутність та зміст понять у сфері інформаційної безпеки

Поняття інформаційної безпеки може розглядатись у широкому та у вузькому розумінні.

Інформаційна безпека (у вузькому розумінні) є необхідною, але невід'ємною складовою інших видів безпеки. Інформаційна безпека – це невід'ємна частина політичної, економічної, військової, соціальної та інших складових національної безпеки. Інформаційна безпека (у вузькому розумінні) розглядається як одна зі складових економічної безпеки, тому що інформація, яка циркулює на підприємстві має комерційний характер і впливає на економічні показники діяльності підприємства (організації). Інформаційна безпека (у вузькому розумінні) розглядається як інформаційна безпека підприємства (організації) – це стан захищеності інформації підприємства (організації) від дестабілізуючого впливу зовнішніх та внутрішніх загроз.

Інформаційна безпека (у широкому розумінні) є самостійним видом безпеки поряд з національною, економічною, військовою, соціальною і політичною. Інформаційна безпека (у широкому розумінні) розглядається як інформаційна безпека держави – це складова національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз.

Інформаційна безпека інформатизації знайшла юридичний вираз на законодавчому рівні у Законі України „Про Національну програму інформатизації" [2]. Відповідно до цього Закону інформаційну безпеку забезпечують:

- комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу;
- комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації;
- банк засобів діагностики, локалізації і профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високо надійні криптографічні методи захисту інформації тощо.

В умовах поширення інформаційних впливів справедливе наступне визначення [3]: „Інформаційна безпека людини, суспільства, держави – це стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів".

Інформаційна безпека розглядається також як єдність концептуальних, теоретичних і технічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної,

соціальної, військової, духовної та ін.), а також сфер формування, циркуляції, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління в усіх видах діяльності тощо.

В організаційно-управлінському аспекті поняття „інформаційна безпека" розглядається як: стан захищеності життєво важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації.

У книзі [4] пропонується наступне визначення поняття „інформаційна безпека". „Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування і розвиток в інтересах громадян, організацій і держави".

За конкретних умов середовища функціонування інформації можна формулювати уточненні визначення, що відповідають цим умовам.

Інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства) – це суспільні відносини щодо створення і підтримання в належному стані режиму нормального функціонування відповідної автоматизованої (комп'ютеризованої) інформаційної системи, систем телекомунікацій; комплекс організаційних, правових та інженерно-технологічних (технічних та програмно-математичних) заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних загроз, реалізація яких може порушити або припинити життєдіяльність конкретної соціо - технічної інформаційної системи.

В іншому випадку: „Інформаційна безпека – це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати збитку власникам або користувачам інформації і підтримуючій інфраструктурі".

Поняття „інформаційна безпека" характеризує стан (властивість) інформаційної захищеності людини, суспільства, природи в умовах можливої дії загроз і досягається системою заходів, спрямованих:

– на попередження загроз. Попередження загроз – це превентивні заходи для забезпечення інформаційної безпеки в інтересах попередження можливості їхнього виникнення;

– на виявлення загроз. Виявлення загроз виражається в систематичному аналізі і контролі можливості появи реальних або потенційних загроз і своєчасних заходів для їхнього попередження;

– на локалізацію злочинних дій і вживання заходів по ліквідації загрози або конкретних злочинних дій;

– на ліквідацію наслідків загроз і злочинних дій та відновлення статус-кво.

У Законі України „Про телекомунікації" під інформаційною безпекою розуміють: „…здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення установленого порядку її маршрутизації" [5].

Як видно з наведених визначень, інформаційна безпека пов'язана із процесом захисту інформації. Тобто, якщо інформація захищена, виходить, що вона в безпеці.

Поняття „захист інформації". Під захистом інформації розуміють сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією [6].

Під захистом інформації, у більш широкому сенсі, розуміють комплекс організаційних, правових і технічних заходів для запобігання загрозам інформаційної безпеки й усуненню їхніх наслідків. Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела є загрозою безпеці інформації.

Мета та методи захисту інформації відображають її сутність. У цьому розумінні захист інформації ототожнюється з процесом забезпечення інформаційної безпеки, як глобальної проблеми безпечного розвитку світової цивілізації, держав, співдружностей людей, окремої людини, існування природи.

Попередження можливих загроз і протиправних дій може бути забезпечене всілякими засобами, починаючи від створення клімату глибоко-усвідомленого відношення співробітників до проблеми безпеки і захисту інформації до створення глибокої, ешелонованої системи захисту фізичними, апаратними, програмними і криптографічними засобами. Попередження загроз можливе і шляхом одержання інформації про протиправні акти, які готуються, плановані розкрадання, підготовчі дії й інші елементи злочинних вчинків. У попередженні загроз важливу роль відіграє інформаційно-аналітична діяльність служби безпеки на основі глибокого аналізу криміногенного стану й діяльності конкурентів і зловмисників.

Виявлення загроз – це дії з визначення конкретних загроз та їхніх джерел, які приносять той або інший вид збитку. До таких дій можна віднести виявлення фактів розкрадання або шахрайства, а також фактів розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів.

Виявлення має на меті проведення заходів щодо збирання, нагромадження й аналітичного оброблення відомостей щодо можливої підготовки злочинних вчинків з боку кримінальних структур або конкурентів на ринку виробництва та збуту товарів і продукції.

Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози і конкретних злочинних вчинків.

Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози.

Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань і забезпечити:

– запобігання розголошення і витоку конфіденційної інформації;

– заборону несанкціонованого доступу до джерел конфіденційної інформації;

– збереження цілісності, повноти і доступності інформації;

– дотримання конфіденційності інформації;

– забезпечення авторських прав.

Найбільш загальними принципами захисту будь-якого виду інформації, що охороняється, є:

– захист інформації організує і проводить власник інформації або уповноважені ним особи (юридичні або фізичні);

– захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, прагне захистити її від незаконного заволодіння і використання на шкоду його інтересам;

– захист інформації здійснюється шляхом проведення комплексу заходів для обмеження доступу до захищеної інформації, що захищається, і створення умов, що виключають або суттєво ускладнюють несанкціонований, незаконний доступ до засекреченої інформації та її носіїв.

Захищена інформація, яка є державною або комерційною таємницею, як і будь-який інший вид інформації, необхідна для управлінської, науково-виробничої та іншої діяльності. Сьогодні перед захистом інформації ставляться більш широкі задачі: забезпечити безпеку інформації. Це обумовлено низкою обставин, і в першу чергу тим, що все більш широке застосування в накопичуванні й обробленні захищеної інформації, одержують електронно обчислювальні машини (ЕОМ), в яких може відбуватися не тільки витік інформації, але і її руйнування, перекручування, підроблення, блокування й інші втручання в інформацію й інформаційні системи.

Отже, під захистом інформації слід також розуміти забезпечення безпеки інформації і засобів інформації, в яких накопичується, обробляється і зберігається захищена інформація.

Таким чином, захист інформації – це діяльність власника інформації або уповноваженої ним особи з:

– забезпечення своїх прав на володіння, розпорядження і управління захищеною інформацією;

– запобігання витоку і втрати інформації;

– збереження повноти, вірогідності, цілісності захищеної інформації, її масивів і програм обробки;

– збереження конфіденційності або таємності захищеної інформації, відповідно до правил, установлених законодавчими й іншими нормативними актами.

Таким чином, захист інформації – це діяльність, яка спрямована на забезпечення конфіденційності, цілісності та доступності інформації в процесі одержання, зберігання, оброблення і поширення за допомогою організаційних, правових, технічних та економічних засобів.

Засоби забезпечення збереження та захисту інформації в державній організації, на підприємстві або фірмі відрізняються за своїми масштабами і формами. Вони залежать від виробничих, фінансових та інших можливостей фірми, від кількості секретів, які вона охороняє та їхньої значимості. При цьому вибір таких заходів необхідно здійснювати за принципом економічної

доцільності, дотримуючись у фінансових розрахунках „золотої середини", оскільки надмірне закриття інформації, так само як і халатне відношення до її збереження, можуть викликати втрату певної частки прибутку або призвести до непоправних збитків. Відсутність у керівників підприємств чіткого уявлення про умови, що сприяють витоку конфіденційної інформації, приводять до її несанкціонованого поширення.

Наявність значної кількості уразливих місць на будь-якому сучасному підприємстві або фірмі, широкий спектр загроз і досить висока технічна оснащеність зловмисників вимагає обґрунтованого вибору спеціальних рішень з захисту інформації. Основою таких рішень можна вважати:

1. Застосування наукових принципів з забезпечення інформаційної безпеки, що включають у себе: законність, економічну доцільність і прибутковість, самостійність і відповідальність, наукову організацію праці, тісний зв'язок теорії з практикою, спеціалізацію і професіоналізм, програмно-цільове планування, взаємодію і координацію, доступність у поєднанні з необхідною конфіденційністю.

2. Прийняття правових зобов'язань з боку співробітників підприємства по відношенню до збереження довірених їм відомостей (інформації).

3. Створення таких адміністративних умов, за яких виключається можливість крадіжки, розкрадання або перекручування інформації.

4. Правомірне залучення до карної, адміністративної й інших видів відповідальності, які гарантують повне відшкодування збитку від втрати інформації.

5. Проведення діючого контролю і перевірки ефективності планування і реалізації правових форм, методів захисту інформації відповідно до обраної концепції безпеки.

6. Організація договірних зв'язків з державними органами регулювання в галузі захисту інформації.

Здійснюючи комплекс захисних заходів головне – обмежити доступ у ті місця і до тієї техніки, де зосереджена конфіденційна інформація (не забуваючи, звичайно, про можливості і методи дистанційного її одержання). Зокрема, використання якісних замків, засобів сигналізації, хорошої звукоізоляції стін, дверей, стелі та підлоги, звуковий захист вентиляційних каналів, отворів і труб, що проходять через ці приміщення, демонтаж зайвої проводки, а також застосування спеціальних пристроїв (генераторів шуму й ін.) серйозно ускладнять або зроблять безглуздими спроби впровадження спецтехніки.

Для надійного захисту конфіденційної інформації доцільно застосовувати наступні організаційні заходи:

1. Визначення рівнів (категорій) конфіденційності інформації, що захищається.

2. Вибір принципів (локальний, об'єктовий або змішаний), методів і засобів захисту.

3. Установлення порядку оброблення захищеної інформації.

4. Облік просторових факторів:

- уведення контрольованих зон;

- правильний вибір приміщень і розташування об’єктів між собою і щодо межі контрольованої зони.

5. Облік тимчасових факторів:

– обмеження часу оброблення захищеної інформації – доведення часу оброблення інформації з високим рівнем конфіденційності до вузького кола осіб.

6. Облік фізичних і технічних факторів:

– визначення можливості візуального (або за допомогою технічних засобів) спостереження відображуваної інформації сторонніми особами;

– відключення контрольно-вимірювальної апаратури від інформаційного об’єкта і її знеструмлення;

– максимальне рознесення інформаційних кабелів між собою і щодо провідних конструкцій;

– їхнє перетинання під прямим кутом.

Для блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів і створення системи захисту об’єкта по них необхідно здійснити низку заходів:

- проаналізувати специфічні особливості розташування будинків, приміщень у будинках, територію навколо них і підведенні комунікації;

- виділити ті приміщення, всередині яких циркулює конфіденційна інформація і врахувати технічні засоби використані в них.

Задача забезпечення інформаційної безпеки у телекомунікаційних мережах загального користування (зокрема в телефонних системах та абонентських мережах) має свої особливості, які розглядаються у наступних розділах даного посібника. Важливість цієї задачі посилюється з розширенням використання центрів обробки викликів та центрів надавання послуг з автоматичним чи напівавтоматичним голосовим спілкуванням з клієнтами.

1.3 Постановка задач проектування

Метою проектування є виконанні етапів та стадій створення комплексної системи інформаційної безпеки (КСІБ) об’єктів інформаційної діяльності (ОІД) телефонних комунікаційних систем (цифрових АТС, центрів оброки викликів) загального користування, які використовуються в органах державної влади місцевого рівня, зокрема в органах внутрішніх справ.

В умовах переходу до постіндустріального та інформаційного суспільства реалізуються програми «Інформатизації», «Електронного уряду», «Електронної демократії». В органах державної влади всіх рівнів створюються «Інформаційно-аналітичні системи» для надавання державних послуг і взаємодії влади з громадянами інформаційного суспільства. Інформаційно-комунікаційні системи є однією з головних і критичних систем органів державної влади, що забезпечують комунікації, об’єднання діючих і нових баз даних, знань, формування і надавання державних послуг.

Інформаційно-аналітична та комунікаційна система (ІАКС) органу державної влади місцевого рівня призначена для забезпечення інформаційної взаємодії органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій.

ІАКС складається із функціональних підсистем, які з точки зору інформаційної безпеки розглядаються як об'єкти інформаційної діяльності (ОІД).

Важливою і необхідною частиною системи Електронного уряду, інформаційно-аналітичної та комунікаційної системи місцевого органу державної влади є система інформаційної безпеки. Для кожного з ОІД створюється комплексні системи інформаційної безпеки (КСІБ).

Захист від несанкціонованого доступу в ОІД реалізується з використанням функціонального профілю захисту (ФПЗ) інформації та загальних механізмів захисту.

Створення та використання КСІБ поділяється на етапи:

- прийняття рішення щодо створення системи інформаційної безпеки;
- розробка Технічного завдання на проектування КСІБ;
- проектування КСІБ згідно вимог Технічного завдання та перед проектних досліджень;
- будівництво, випробування, атестація, державна експертиза та здавання КСІБ до експлуатації;
- технічна експлуатація та вдосконалення КСІБ;
- виведення з експлуатації та утилізація КСІБ.

Кожен етап виконується у декілька стадій.

Для обраного ОІД необхідно виконати наступні стадії проектування КСІБ:

1. Провести аналіз фізичної і логічної архітектури ІАКС органу державної влади та систем автоматизованої обробки інформації, що використовуються в системі. Провести опис інформаційних ресурсів ІАКС.
2. Проаналізувати інформаційну модель ІАКС. Дати опис інформаційних потоків, інтерфейсів між користувачами, споживачами і суб'єктами ІАКС.
3. Провести аналіз архітектури та інформаційних ресурсів заданого ОІД комунікаційної системи.
4. Розробити модель ОІД за своїм варіантом з позицій інформаційної безпеки. Скласти перелік та провести категоріювання інформації, яка підлягає захисту в ОІД.
5. Виявити і провести аналіз уразливих елементів основних і додаткових технічних засобів та систем обробки інформації ОІД за своїм варіантом.
6. Визначити перелік загроз і провести аналіз можливих каналів витоку інформації ОІД за своїм варіантом. Проаналізувати інформаційне, фізичне, обчислювальне середовище, середовище користувачів та персоналу.
7. Розробити структурну схему КСІБ ОІД.
8. Розробити політику безпеки інформації та План захисту інформації в заданому ОІД.
9. Обрати і обґрунтувати вибір функціонального профілю захисту, рівня гарантій захисту.

10. Сформувати перелік детальних вимог до системи захисту інформаційних ресурсів ОІД за своїм варіантом, які необхідно реалізувати відповідно до класів захищеності:

- вимоги до фізичних, організаційних, організаційно-технічних загальних заходів захисту;
- вимоги до комплексу технічних засобів захисту інформації (КТЗІ) в частині захисту від витоку технічними каналами;
- вимоги до КСЗІ в частині захисту від несанкціонованого доступу (НСД) з підвищеними вимогами до цілісності та доступності інформації;
- вимоги до криптографічної підсистеми захисту – алгоритми шифрування та електронного підпису;
- вимоги до гарантій захисту на основі вибраного критерію гарантій;

11. Сформувати перелік послуг та механізмів захисту, які необхідно реалізувати в ОІД відповідно до класів захищеності

12. Провести експертну оцінку поточного рівня безпеки.

13. Визначити інформаційні ризики у разі здійснення загроз ОІД згідно свого варіанту.

14. На основі розробленої політики безпеки інформації описати специфікації (політку кожної з послуг ФПЗ) функціонального профілю захисту інформації в ОІД за своїм варіантом.

15. Скласти опис послуг і механізмів безпеки в системі захисту інформаційних ресурсів заданого ОІД, які необхідно реалізувати відповідно до класів захищеності:

- опис реалізації послуг і механізмів безпеки фізичних, організаційних, організаційно-технічних загальних заходів захисту;
- опис реалізації послуг і механізмів безпеки комплексу технічних засобів захисту інформації (КТЗІ) в частині захисту від витоку технічними каналами;
- опис реалізації послуг і механізмів безпеки КСЗІ в частині захисту від несанкціонованого доступу (НСД) з підвищеними вимогами до цілісності та доступності інформації;
- опис реалізації послуг і механізмів безпеки криптографічної підсистеми захисту – алгоритми шифрування та електронного підпису;

16. Описати специфікації реалізованих гарантій захисту згідно обраного рівня гарантій захисту.

17. Розробити алгоритм і програму заданого механізму безпеки.

18. Сформувати перелік детальних вимог до системи захисту інформаційних ресурсів заданого ОІД, які необхідно реалізувати відповідно до класів захищеності:

- вимоги до засобів захисту периметру ІАС – між мережних екранів, фільтрів тощо;
- вимоги до підсистеми виявлення атак, збоїв та ліквідації їх наслідків;
- вимоги до управління інформаційною безпекою ІАС та підсистеми моніторингу інформаційної безпеки;
- вимоги до аудиту інформаційної безпеки.

19. Провести оцінювання досягнутого рівня безпеки

20. Розробити план заходів з підготовки до проведення атестації комплексу технічного захисту інформації (КТЗІ) та державної експертизи КСЗІ в ОІД.

Об’єктами інформаційної діяльності в комунікаційній системі є: цифрова (відомча) АТС заданого типу, центр обробки викликів, центр надавання державних послуг, центр управління комунікаціями тощо.

Запитання для самоконтролю

1. Як інформаційна безпека пов’язана з економічною, національною та глобальною безпекою?

2. Дайте визначення поняття «інформаційна безпека» у широкому і вузькому смислі.

3. Сформулюйте поняття «захист інформації».

4 Перелічіть загальні принципи захисту інформації.

5 Які можуть бути спеціальні рішення із захисту інформації

6 Які організаційні заходи доцільно застосовувати для надійного захисту конфіденційної інформації.

7 Що є метою проектування у виконанні етапів та стадій створення комплексної системи інформаційної безпеки (КСІБ).

8 Які є етапи створення та використання КСІБ?

2 КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В ПРОГРАМНО-КЕРОВАНИХ АТС

Згідно нормативного документа [8] об'єктом технічного захисту на програмно-керованих АТС, а також на відомчих, корпоративних АТС є конфіденційна, а також відкрита важлива для особи, суспільства і держави інформація, яка зберігається та циркулює на цих АТС.

Передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності комплексної системи захисту інформації вимогам із захисту інформації.

У цьому розділі розкриваються основні принципи й напрямки забезпечення інформаційної безпеки у відповідності з задачами та функціями ЦАТС, які базуються на нормативно-правових документах України, відповідають вимогам щодо забезпечення конституційних прав людини, проведення заходів із захисту даних споживачів при автоматизованій обробці інформації, захисту засобів телекомунікацій і інформації, що передається телекомунікаційними мережами.

Нормативно-правову базу системи захисту інформації в програмно-керованих АТС складають Закони та держстандарти України, комплект НД ТЗІ [9…16] тощо.

2.1 Модель цифрового вузла комутації з позицій технічного захисту інформації

Для надання послуг якісного, надійного, безпечного телефонного зв'язку має бути сформована надійна захищена інфраструктура ЦАТС та ліній телекомунікацій з використанням доступних та ефективних засобів і способів інформаційного захисту. Розрізнені заходи щодо інформаційної безпеки, які приймаються при забезпеченні якості послуг, ефективності технічної експлуатації та управління ЦАТС необхідно привести у єдину керовану комплексну систему інформаційної безпеки, яка має забезпечити:

- стійке функціонування ЦАТС та мережі телекомунікацій;
- попередження загроз їхній безпеці;
- захист законних інтересів підприємства від протиправних посягань;
- недопущення крадіжки фінансових засобів, розголошення, утрати, спотворення й знищення службової, технологічної, управлінської інформації;
- ефективну виробничу діяльність усіх підрозділів;
- підвищення якості наданих послуг та гарантії безпеки майнових прав та інтересів абонентів.

Згідно нормативно-правової бази *технічний захист інформації спрямований на забезпечення*:

- порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, що є об'єктом державної власності та охороняється згідно із законодавством;
- захисту, спрямованому на недопущення блокування інформації, що є державними інформаційними ресурсами, несанкціонованого ознайомлення з

нею та/або її модифікації і, в тому числі, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

- захисту від несанкціонованого доступу (НСД) до державних інформаційних ресурсів з боку мереж передачі даних, зокрема, глобальних мереж.

- порядку доступу, цілісності та доступності комерційної та відомчої конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в державних органах, підприємствах, установах та організаціях;

- захищеності відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює.

Конфіденційність інформації, яка є державним інформаційним ресурсом, під час передавання мережею забезпечує власник автоматизованої системи або оператор мережі передачі даних за договором із власником автоматизованої системи.

Заходи щодо технічного захисту конфіденційної інформації, що не належить державі, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних органів, підприємств, установ і організацій, встановлюються власником інформації або розпорядником.

Узагальнена модель інфраструктури цифрового вузлу комутації з позицій технічного захисту інформації показана на рис. 2.1.

Обладнання ЦАТС поділяють на станційну частину, блоки абонентських виносів (БАВ) і мережу абонентських, з'єднувальних та міжстанційних цифрових та аналогових ліній, які є для порушника об'єктами несанкціонованого доступу до них, до інформації, що ними передається, і впливу на їх працездатність. На лініях може бути обладнання, встановлене порушником (ОВП).

Станційна частина виконує функції опорної станції або опорно-транзитної станції і з'єднана з іншими станціями міжстанційними з'єднувальними, а з блоками абонентського виносу – з'єднувальними цифровими лініями Е1 з потрібним числом підсилювальних та регенеративних ділянок. БАВ приєднується до опорної станції, як правило, за інтерфейсом *V*3.1, *V*3.2.

У якості міжстанційних з'єднувальних ліній можуть використовуватись цифрові канали *E*1 з магістральної мережі *SDH* чи *ATM*.

Станційна частина цифрового вузла комутації має у своєму складі:

- підсистему комутації абонентських і з'єднувальних ліній (КАЗЛ);

- управляючий комплекс вузла комутації (УК) з автоматизованими робочими місцями операторів (АРМ оператора);

- підсистему технічної експлуатації (СТЕ) вузла комутації, що дублюється у центрі технічної експлуатації цифрових вузлів комутації, звідки здійснюється віддалений контроль та управління вузлами.

Станційна частина цифрового вузла комутації взаємодіє з наступними технологічними мережами:

АСКР – автоматизована система контролю та розрахунків з абонентами для тарифікації наданих телефонних послуг;

TMN – мережа управління електрозв'язком для технологічного контролю та адміністративно-бізнесового менеджменту послуг;

IN – мережа надання інтелектуальних послуг;

*SS*7 – система сигналізації для управління процесом з'єднання;

СС - система синхронізації для отримання опорних тактових частот.

У станційній частині можуть бути виявлені програмні закладки та апаратні закладні пристрої, які виконують не документовані функції і не контролюються системою технічної експлуатації вузла комутації.

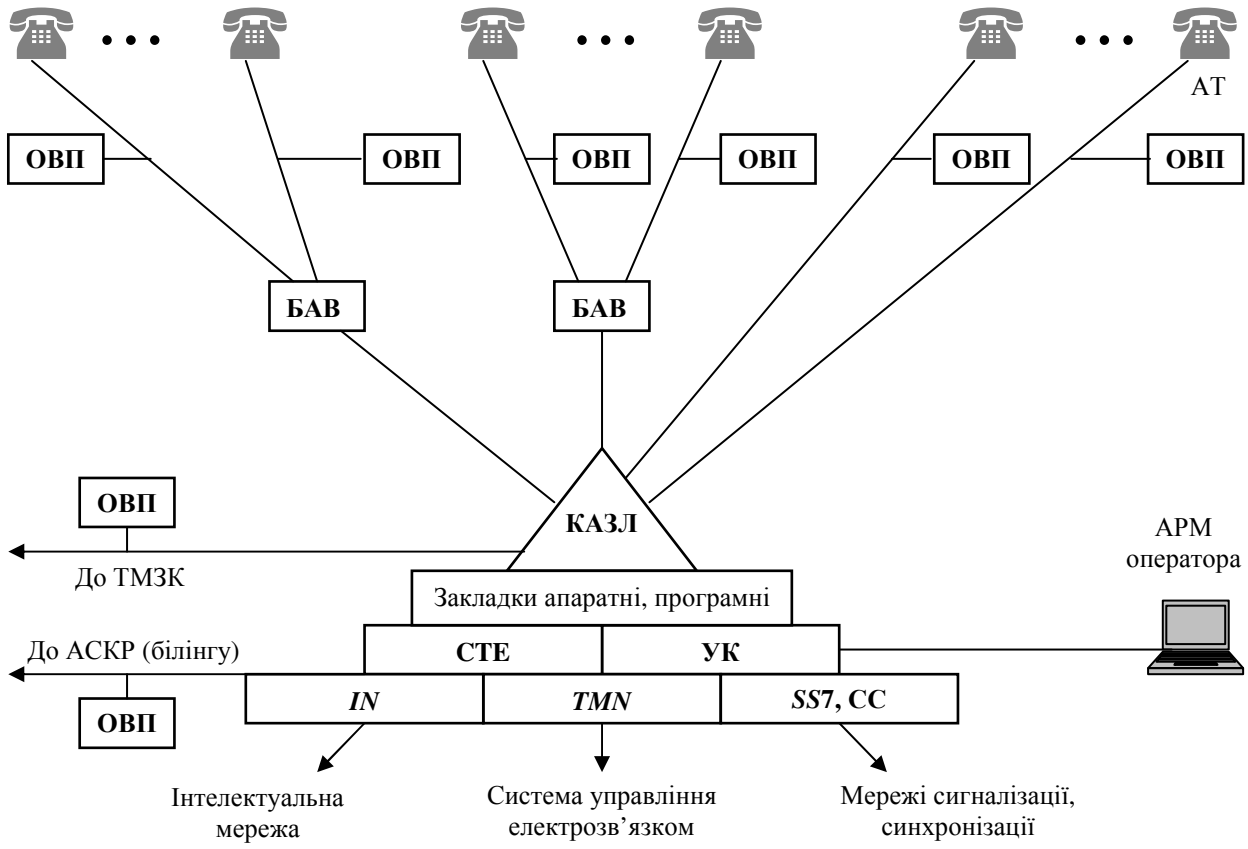

Рисунок 2.1 – Модель інфраструктури цифрового вузла комутації з позицій захисту інформації

Позначення: **АРМ** (💻) – автоматизоване робоче місце; **АСКР** – автоматизована система комплексних розрахунків з абонентами; **АТ** – абонентські термінали; **БАВ** – блок абонентського виносу; **КАЗЛ** – підсистема комутації абонентських та з'єднувальних ліній; **ОВП** - обладнання, встановлене порушниками; **СС** – система синхронізації; **СТЕ** – система технічної експлуатації; **ТМЗК** – телекомунікаційна мережа загального користування; **УК** – управляючий комплекс; ***IN*** - інтелектуальна мережа; ***TMN*** - мережа управління телекомунікаціями; ***SS*7** - система сигналізації № 7.

Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ наведена на рис. 2.2 [8].

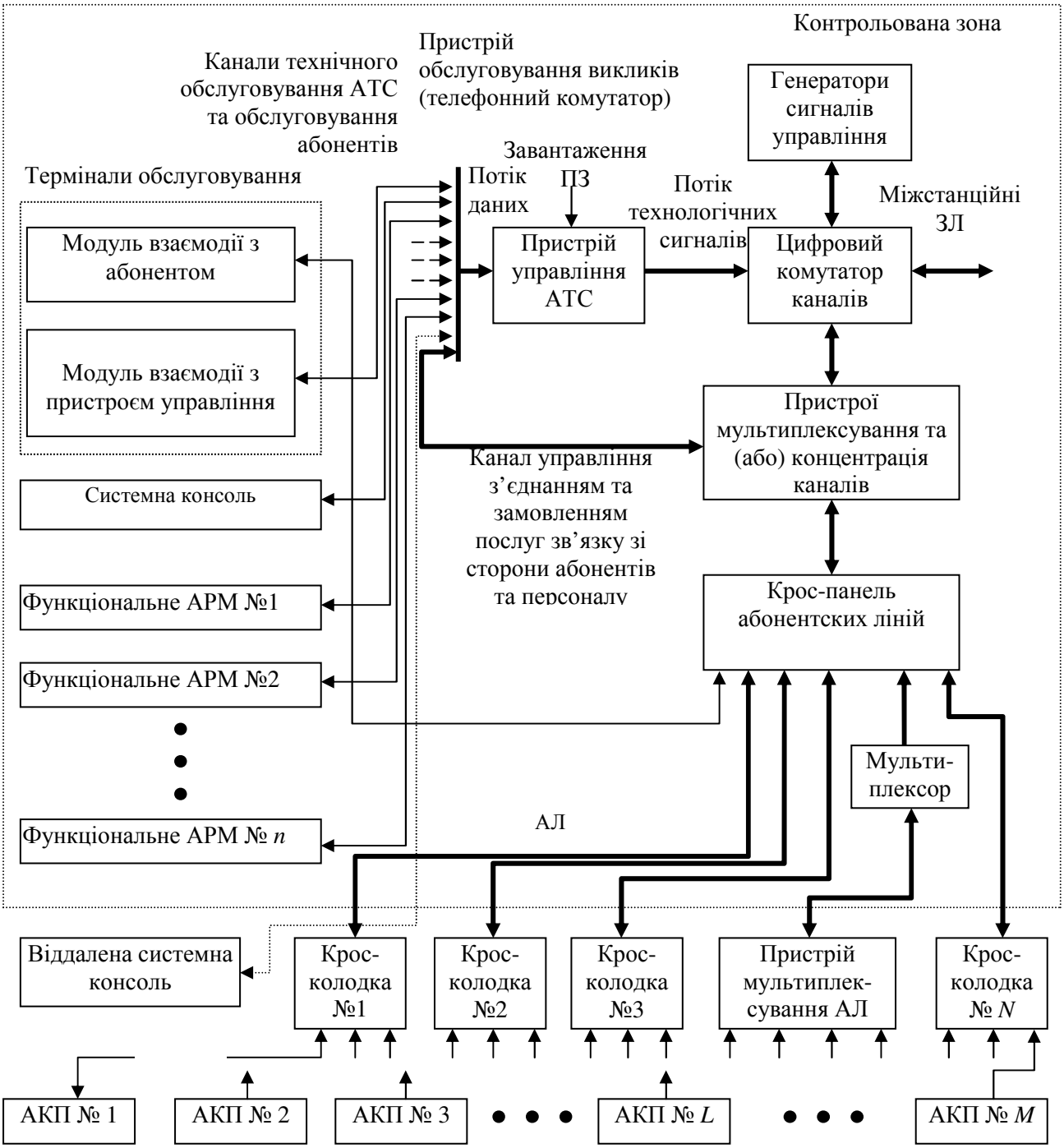

Рисунок 2.2 – Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ (з НД ТЗІ 1.1-001-99)

Позначення: **АКП** – абонентські кінцеві прилади (апарати); **АЛ** – абонентські лінії; **АРМ** – автоматизоване робоче місце; **АТС** – автоматична телефонна станція; **ЗЛ** – з'єднувальні (міжстанційні) лінії; **ПЗ** – програмне забезпечення; ***L*** – поточне число АКП; ***M*** – загальна кількість АКП (ємність станції); ***N*** – кількість кросових колодок; ***n*** – кількість АРМ; контрольована зона – територія, де унеможливлюється присутність сторонніх осіб.

Схемою виділяються ті елементи станції, які мають безпосереднє відношення до процесів захисту інформації.

Станційне обладнання ЦАТС розміщується на охороняємому об'єкті, де проводиться повний цикл організаційно-технічних заходів з комплексної інформаційної безпеки певного атестованого рівня.

Обладнання програмно - керованих АТС має захищеність базового рівня, яка забезпечується фірмою-виробником даного обладнання.

При встановленні обладнання на мережу рівень захищеності знижується за рахунок можливого впливу на саму систему зі сторони мережі каналами абонентського доступу, сигналізації, синхронізації, тарифікації і системи управління з віддалених терміналів.

Підсистема управління станцією містить у собі:

- спеціалізовані пристрої управління, що реалізують принцип програмного управління і складаються, здебільшого, з процесорів, пристроїв внутрішньої і зовнішньої пам'яті, периферійних пристроїв, спеціалізованих модулів управління сигналізацією, опрацювання викликів, надання послуг і деяких інших програмно-апаратних компонентів, які є характерними для комп'ютерної техніки;

- термінали обслуговування, що приєднані до пристроїв управління через канали технологічного обслуговування АТС і до підсистеми КАЗЛ - через канали інформаційного обслуговування абонентів.

Підсистема КАЗЛ містить у собі пристрої, що реалізують процеси комутації, мультиплексування та концентрації абонентських і міжстанційних з'єднувальних ліній, а також компоненти устаткування абонентських ліній зв'язку - абонентські прикінцеві пристрої, фізичні лінії зв'язку, пристрої мультиплексування абонентських ліній, станційні абонентські комплекти тощо.

На виходах підсистеми управління утворюються в реальному часі потоки технологічних сигналів, за допомогою яких має місце процес управління підсистемою КАЗЛ. З іншого боку, абонентські прикінцеві пристрої мають можливість обмінюватися керуючою інформацією з підсистемою управління станцією через канали управління з'єднаннями й замовлення послуг.

Незалежність підсистем управління станцією і КАЗЛ розуміється в тому сенсі, що підмножина загроз для інформації, яка характерна для підсистеми управління станцією, не перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ, за передумовою відсутності механізмів реалізації загроз на підсистемі управління з боку підсистеми КАЗЛ і, навпаки, - на підсистемі КАЗЛ з боку підсистеми управління станцією.

Коректність такої декомпозиції структури програмно-керованих АТС обумовлена прийнятими щодо них проектними рішеннями, що не передбачають:

- можливостей штатних впливів на підсистему управління станцією з боку абонентських прикінцевих пристроїв, за винятком можливості запуску абонентом задач із фіксованого набору, що реалізують заздалегідь передбачені функції замовлення абонентом додаткових видів послуг, які надаються станцією;

- можливостей штатних впливів на інформацію в розмовних трактах із боку підсистеми управління станцією, за винятком можливості штатних приєднань

до вже встановлених з'єднань (наприклад, із боку телефонного комутатора або абонентських прикінцевих пристроїв у режимі конференц зв'язків), однак з обов'язковим оповіщенням учасників розмови про всі додаткові підключення до їхніх розмовних трактів (зокрема, фоновими тональними сигналами).

Відносність незалежності вищезгаданих підсистем розуміється в тому сенсі, що за певних умов внаслідок помилок або некоректних (зокрема, зловмисних) дій, які були допущені на передексплуатаційних стадіях життєвого циклу АТС (наприклад, при установці програмних закладок або апаратних закладних пристроїв), або внаслідок якісної недостатності АТС, однак, можливі реалізації загроз на підсистемі управління з боку підсистеми КАЗЛ, і, навпаки, - на підсистемі КАЗЛ з боку підсистеми управління станцією.

Далі розглянемо загрози інформації та моделі порушників, які їх здійснюють.

2.2 Загрози для інформації та моделі порушників

2.2.1 Основні загрози інформаційним ресурсам вузла комутації.

В інформаційній сфері України відокремлені загрози національній безпеці:

- прояви обмеження свободи слова та доступу громадян до інформації;
- комп'ютерної злочинності та комп'ютерного тероризму;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення невірогідної, неповної або упередженої інформації.

Передумовами можливого витоку інформації, порушення її цілісності, блокування та НСД, безконтрольного та неправомочного доступу до інформації та її використання є:

- комунікаційне обладнання іноземного виробництва, яке використане у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються. Використання великої кількості засобів зв'язку іноземного виробництва створює можливість втручання іноземних спецслужб в роботу мереж зв'язку шляхом руйнування програмних засобів в певний момент або створення каналів несанкціонованого впливу на інформацію, а також приводить до зростання залежності операторів зв'язку від закордонних виробників програмно-апаратних засобів зв'язку. В закордонній апаратурі можуть бути "закладки" додаткових, не відображених в технічних характеристиках режимів роботи. Активізація таких режимів може здійснюватись як випадково, в процесі роботи оператора, так і дистанційно порушником, що приводить до втрати або зміни даних, помилок у програмному забезпеченні або паралельному підключенні до каналів;

- прогрес у різних галузях науки і техніки призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації вітчизняного та іноземного виробництва з метою здобування, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо, радіотехнічної, оптико-електронної, теплової, акустичної, хімічної, магнітометричної та радіаційної розвідок;

- злочинна діяльність, спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;

- діяльність громадських формувань, політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб спрямована на одержання переваги у політичній боротьбі та конкуренції;

- розміщення на державних та спільних об'єктах зв'язку технологічного обладнання спільних підприємств та представництв інофірм, що вимагає проведення додаткових заходів із забезпечення вимог ТЗІ;

- зростання зацікавленості іноземних розвідок питаннями промислової, комерційної діяльності, ресурсів в Україні.

- відсутність системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- відсутність політики безпеки систем комутації та телекомунікаційних мереж, де б формулювались вимоги щодо захисту від загроз працездатності, підтримання режиму конфіденційності та відсутності несанкціонованого доступу.

- нелегальне використання ресурсів операторів для несанкціонованого надання послуг зв'язку, що знижує доходи останніх;

- різні фрагменти мережі експлуатуються різними операторами з різними формами власності.

Загрози інформаційній безпеці є при забезпеченні:

1) конфіденційності:
   - крадіжка (копіювання) інформації та засобів її обробки;
   - утрата (ненавмисна утрата, витік) інформації та засобів її обробки;
2) доступності:
   - блокування інформації;
   - знищення інформації та засобів її обробки;
3) цілісності:
   - модифікація (спотворення) інформації;
   - заперечення справжності інформації;
   - нав'язування хибної інформації.
4) спостережності:
   - блокування;
   - модифікація інформації;
   - маскування інформації;
5) порядку маршрутизації трафіка:
   - крадіжка трафіка;

- несанкціоноване використання послуг та інформаційних ресурсів телекомунікаційних мереж.

Детально загрози інформаційній безпеці, саме вузлів комутації, а також перелік інформації, яка захищається, наведені в КНД 45-164-2001 [15].

Джерела загроз інформаційній безпеці поділяють на три групи.

1. Обумовлені зловмисними чи випадковими діями суб'єкта (антропогенні джерела загроз).

2. Обумовлені технічними засобами (техногенні джерела загроз).

3. Обумовлені природними стихійними джерелами.

До антропогенних джерел загроз відносять

1. Зовнішні антропогенні джерела загроз:

- кримінальні структури;
- потенційні злочинці та хакери;
- недобросовісні партнери, конкуренти, представники сторонніх організацій, відвідувачі;
- технічний персонал постачальників;
- представники організацій нагляду та аварійних служб;
- представники силових структур.

2. Внутрішні антропогенні джерела загроз:

- основний персонал (користувачі-оператори, системні і прикладні програмісти, розробники, оператори баз даних, оператори вводу даних);
- представники служби захисту інформації (системні і мережні адміністратори, адміністратори безпеки);
- керівництво;
- технічний персонал (життєзабезпечення, експлуатації);
- допоміжний персонал (прибиральники, охорона);
- співробітники, звільнені з роботи.

Особливу групу внутрішніх антропогенних джерел загроз складають особи з порушеною психікою, впроваджені та завербовані агенти (іноземні агенти, що збирають інформацію, корпоративні розвідники) з числа основного, допоміжного та технічного персоналу, представників служби захисту інформації.

До техногенних джерел загроз відносять

1. Зовнішні техногенні джерела загроз:

- засоби службового зв'язку;
- мережі інженерних комунікацій (водопостачання, каналізації, вентиляції);
- засоби пожежної, охоронної сигналізації;
- транспорт;

2. Внутрішні техногенні джерела загроз:

- неякісні технічні засоби комутації та обробки інформації;
- неякісні програмні засоби управління та обробки інформації;
- допоміжні засоби;
- інші технічні засоби, що застосовуються в ЦАТС.

Природними зовнішніми джерелами загроз є пожежі, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, різні непередбачені обставини, не пояснювані явища, інші форс-мажорні обставини: різні рішення вищих державних органів, забастовки, війни, революції тощо.

При складанні окремої моделі порушника орієнтуються на конкретний об'єкт захисту, враховують мотиви дій і соціально-психологічні аспекти порушення, потенційні можливості у доступу до інформаційних ресурсів різних категорій зовнішніх та внутрішніх порушників на різних просторово-часових зрізах об'єкта захисту.

2.2.2 Модель порушника безпеки

Детальну класифікацію моделей порушників антропогенного типу, їх рівні можливостей, основні способи реалізації загроз для інформації програмно-керованих АТС наведено у НД ТЗІ 1.1.001-99 [8]. Класифікація проводиться за рівнем можливостей, котрий надається їм штатними засобами. Виокремлено чотири рівні можливостей порушення НСД:

1 (найнижчий рівень можливостей) – запускання програм (задач) із фіксованого набору, котрий реалізує передбачені функції щодо обробки інформації. Це обслуговуючий персонал, котрий забезпечує експлуатацію обладнання ЦАТС. Інженери-електронники ЦАТС, користуючись автоматизованим робочим місцем (АРМ) та комутаційною системою, можуть мати доступ до інформації абонента. Вони мають можливість приєднувати до ЦАТС закладні пристрої.

2 – можливість створювання та запускання власних програм з новими функціями щодо обробки інформації. Це оператори даного або інших вузлів комутації. Користуючись комплектом або модулем з'єднувальної лінії, вони мають доступ до програмного забезпечення (ПЗ) АРМ, функціонального й спеціалізованого ПЗ та до баз даних. Типові можливості полягають у передаванні сигналів, як передбачених, так непередбачених у відповідних інтерфейсах.

3 – можливість управління роботою обчислювального комплексу, тобто можливість впливу на базове ПЗ ЦАТС та на склад і конфігурацію обладнання. Це оператори ЦАТС. Користуючись АРМ, вони мають доступ до баз даних, ПЗ АРМ, функціонального й спеціалізованого ПЗ та інформації абонентів. Типові можливості такого порушника: формування штатних команд, запускання задач, не задекларованих у технічній документації, несанкціоноване приєднання до інформаційних трактів.

4 – весь обсяг можливостей суб'єктів, здійснюючих проектування, реалізацію та ремонт технічних засобів, до залучення у склад обладнання власних технічних засобів з новими функціями. Це програмісти, котрі беруть участь у розробленні й виготовленні ВК. Користуючись АРМ і пристроями управління, вони здатні впливати на функціональне та спеціалізоване ПЗ і на ПЗ АРМ. Типові можливості є такі: впровадження програмних закладок, впровадження шкідливих кодів (вірусів), помилки у ПЗ та комутаційній системі.

Якщо на вузлі комутації нема програмних та апаратних закладок, то звичайний абонент мережі практично не має можливості впливати на управляючу систему телефонної станції. Регламентовані для цифрових та аналогових терміналів користувача основні й додаткові послуги не можуть впливати на роботу управляючого комплексу у цілому. Абонент може діяти лише через абонентський комплект. Він здатен активізувати програмне закладення, дістати інформацію інших абонентів через несправності обладнання ЦАТС.

Продовжимо розгляд загроз інформації від зовнішніх, по відношенню до ЦАТС, джерел.

Загрози інформаційній безпеці можуть бути різноманітними і довільного походження за часом, тривалістю, факторами та наслідками.

Зрив роботи ЦАТС можливий при зупинці системи електроживлення або виведенні її з ладу порушником.

Можливе впровадження "вірусу" – мікропрограми, здатної самостійно розмножуватись і поширюватись у мережі.

Пристрої обробки інформації, котрі є складовою частиною цифрового вузла комутації, це ЕОМ зі стандартною архітектурою, для яких можна створювати засоби нападу, віруси тощо.

Можливості стосовно здійснення загроз залежать від місцезнаходження порушника. Якщо порушник перебуває поза межами ЦАТС, то його можливості залежать від того, чи є засоби захисту інформації у системі тарифікації (припускається чи не припускається віддалене приєднання легальних користувачів до системи тарифікації), засоби безпеки при виході на мережу *SS*-7 та *TMN*, при приєднанні до Інтернет.

Якщо таких засобів захисту нема, то можливі впливи порушника через зовнішні інтерфейси обладнання, системи сигналізації на абонентських та з'єднувальних лініях.

Загрози стосовно захищеності збільшуються при інтеграції у цифрові комплекси нових функцій, а саме: часткова (приватна) віртуальна мережа (*VPN*), що забезпечує внутрішній офісний зв'язок та зв'язок з філіалами; функції білінгу на базі локальної мережі; вихід на глобальну мережу – Інтернет, а також використання на мережі імпортних програмно-апаратних комплексів.

Існує небезпечна загроза крадіжки трафіка при сумісному використанні системи зв'язку різними операторами. Захист досягається використанням міжмережних екранів, шлюзів по каналам управління, синхронізації та сигналізації, здійснення контролю трафіка і тарифікації.

2.2.3 Загрози інформаційним ресурсам ЦАТС від приєднаних технологічних мереж

У межах контрольованої зони ЦАТС може встановлюватись різноманітне устаткування телекомунікаційних мереж. Частина цього обладнання приєднується безпосередньо до обладнання ЦАТС і може впливати на її роботу. Зокрема, це система сигналізації й синхронізації, система централізованого

управління та технічної експлуатації, з'єднувальні та абонентські лінії, системи передавання до АСКР тощо.

Можливі варіанти інформаційного нападу на мережі зв'язку. Мережа зв'язку складається з вузлів комутації та систем передачі і її можна розглядати, як програмну інформаційну систему з безліччю зовнішніх зв'язків. Розглядають такі загрози:

- загроза атаки через АРМ адміністратора;
- загроза несанкціонованого входу в АРМ адміністратора;
- загроза модифікації системного або програмного забезпечення адміністрування вузла зв'язку;
- загроза зараження файлів комп'ютерними вірусами;
- загроза прослуховування та модифікація трафіка;
- загроза модифікації апаратної частини АРМ, АТС, *SS*7 і лінійної апаратури (вставка чужого пристрою);
- загроза відмови в обслуговуванні;
- загроза атаки через систему віддаленого програмування і діагностики;
- загроза атаки через систему сигналізації та управління;
- загроза атаки наведеним сигналом;
- загроза атаки абонентськими лініями;
- загроза атаки через мережу електроживлення;
- загроза атаки через системи тарифікації і записи переговорів;

Ці загрози розділяють на загрози на рівні програмного забезпечення, апаратної частини, середовища розробки і середовища експлуатації;

Більшість загроз на системи зв'язку складають атаки на програмному рівні. Тому необхідно відслідковувати можливість входу у систему програмування або управління системами зв'язку.

Входи в програмне забезпечення АТС і системи передачі можуть бути легальними і нелегальними. До легальних входів відносяться зв'язок з системою віддаленого програмування і діагностики та з локальною системою програмування і тарифікації.

Решта входів - нелегальні. При цьому у сучасних АТС вхід віддаленого програмування може бути заблоковано парольним захистом або фізичним відключенням. В інтелектуальних мережах вказаний вхід функціонує і відключений бути не може. За рівнем небезпечності ці загрози можна розділити на такі основні рівні:

а) найбільш небезпечним є вхід віддаленого програмування та діагностики АТС, який функціонально призначено для безпосереднього втручання в програмне забезпечення систем зв'язку. Наслідки такого втручання можуть бути будь-якими, навіть до зупинки системи або мережі зв'язку. При цьому неможливо оперативно усунути причину збою системи та усі неполадки, оскільки нема можливості здійснити протоколювання усіх дій зі сторони віддаленого доступу в систему управління;

б) вхід локального програмування і тарифікації також небезпечний для програмного забезпечення, але доступ до нього обмежено персоналом станції і безпека може бути забезпечена організаційними заходами. Втручання може

бути легко визначене при дотриманні усіх вимог експлуатації: дії обслуговуючого персоналу завжди протоколюються;

в) напад абонентськими і з'єднувальними лініями, а також зі сторони системи сигналізації може бути проведено через активізацію "закладок", що відкривають по кодовому сигналу доступ до ПЗ АТС і систем передачі з вказаних напрямків. Закладки можуть бути створені на програмному та апаратному рівнях;

г) напад наведеним сигналом (наприклад, з космічного об'єкта) може бути здійснено через апаратні «закладки» разом з програмними «закладками». Можуть бути направлені на виведення обладнання з ладу застосуванням потужних електромагнітних імпульсів;

д) може бути "внутрішній" напад, який забезпечено закладкою у ПЗ, що спрацьовує від лічильника, дати або інших внутрішніх факторів.

Крім того, практично все існуюче ПЗ систем передачі має обмеження за часом. По закінченні часу підтримки даної версії необхідно або купувати нову або експлуатувати стару на свій страх і ризик.

Загрози, що реалізуються через систему сигналізації. Застосування сигналізації *SS*7 дозволяє здійснювати певні функції управління окремими вузлами зв'язку, при якому може бути нанесена значна шкода оператором зв'язку.

Системи сигналізації забезпечують передавання різноманітних сигналів управління, в тому числі цифр номера, які через функціональні елементи комутаційної системи надходять для аналізу в управляючий комплекс. В цьому разі можливі різні варіанти використання сигналів управління для активізації програмних закладок, наприклад таких:

- використання режиму типу "додаткова послуга", котра не декларується в документації;
- використання абонентського номера чи коду для активації програмної закладки;
- певні короткочасні маніпуляції з абонентською трубкою.

Система сигналізації *SS*7, крім вищезазначених можливостей, потенційно надає додаткові можливості організації НСД. У складі *SS*7 є підсистеми забезпечення можливостей транзакцій (*TCAP*) та прикладних підсистем, котрі організуються на них, такі як підсистема рухомого зв'язку *GSM* (*MAP*), підсистема інтелектуальних мереж (*INAP*), підсистема експлуатації, техобслуговування, адміністрування й управління (*OMAP*) та інші. До загроз від застосування *SS*7 також належать:

- інтерфейси, спеціалізовані для нетелефонних функцій (*TCAP*, *OMAP* тощо) системи *SS*7, можуть бути використані для прихованого введення команди, котра реалізує несанкціонований вплив на ЦАТС;
- в *SS*7 організовується доступ до мережних баз даних. Виникає загроза їхнього навмисного спотворення, що може спричинити порушення роботи мережі.

Для захисту від можливого впливу необхідно здійснювати фільтрацію загальноканальної сигналізації та протоколювання повідомлень.

Загрози, що реалізуються за допомогою системи централізованого управління. Якщо порушник перебуває всередині ЦАТС, то, навіть якщо наявні засоби безпеки при реалізації систем тарифікації, засоби безпеки при виході на мережу *SS*7 та TMN, засоби захисту за приєднанні до Інтернету, то він має багато можливостей для здійснення загроз. Порушник з правами оператора УК може здійснювати НСД шляхом формування штатних команд, запускати програми, нерегламентовані в технічній документації. Порушення доступу відбувається в разі:

- модифікації баз даних (встановлення несанкціонованих режимів технічної експлуатації та видів обслуговування);
- ознайомлення з конфіденційною інформацією баз даних (адресами вхідних та вихідних з'єднань, часом встановлення з'єднання, режимами зв'язку, додатковими використовуваними видами обслуговування);
- зупинки та перезапускання ЦАТС (порушення зв'язку);
- заміни ПЗ (нове інстальоване ПЗ може мати програмні закладення та люки).

Основні можливі варіанти захисту при забезпеченні захисту від впливу через систему управління, як самої критичної ланки, це впровадження жорсткого розмежування прав доступу до інформаційних ресурсів, як на фізичному, так і на програмному рівнях, адміністрування і протоколювання усіх операцій.

Найбільш підпадають під загрози ПЗ АРМ, якщо вони функціонують на базі ПЕОМ і використовують для роботи операційну систему *Windows* чи *MS-DOS*. Функціональне та спеціалізоване ПЗ, як правило, зашите у постійні запам'ятовувальні пристрої. Проникнення в операційну систему вузла комутації вважається практично неможливим.

Оскільки найгірший результат нападу - це руйнування системи зв'язку в цілому або окремих її фрагментів, то в цифрових АТС і системах цифрової передачі даних *SDH*, *PDH* (радіорелейних, кабельних, волоконно-оптичних) найбільш вразливим елементом являється програмне забезпечення, яке піддається нападу в першу чергу. При цьому, захистивши програмне забезпечення від несанкціонованого втручання, з достатньою ймовірністю забезпечується цілісність мережі та її елементів.

Оскільки сучасне обладнання цифрового зв'язку базується на комп'ютерних технологіях, питання забезпечення інформаційної безпеки найбільш ефективніше можуть бути вирішені спеціалістами з обчислювальної техніки, які мають відповідний досвід.

Загрози на абонентських та з'єднувальних лініях. Стосовно абонентських, з'єднувальних та міжстанційних ліній зв'язку виділяють:

- загрози від випадкових дій (впливів) порушників;
- загрози від зловмисних дій порушників;
- загрози безпеці.

Аварії можуть бути викликані впливами техногенного (результаті земляних та будівельних робіт в районах кабельних трас, розбою та зловмисної диверсійної діяльності) чи природного характеру (промерзання та деформація кабелю у зимовий період). Інформаційна безпека підтримується чіткою

стандартною плановою організацією ремонтно-відновлювальних робіт та прогнозуванням ресурсів, необхідних для ліквідації наслідків аварії.

В лінійних трактах, на їх елементах порушник може успішно здійснювати тривалий практично не виявляємий НСД до інформації за допомогою спеціальних засобів доступу до аналогових і цифрових каналів, здійснювати виведення на запис, прослуховування або ретрансляцію несанкціоновано одержаних даних та мови. Захист в такому разі здійснюється плановим патрулюванням (пішим чи моторизованим) кабельних трас та посиленням контролю в періоди вирішення важливих задач. Часто застосовують шифрування інформації.

Загрози інформації в цифрових системах передачі. Цифрові системи передавання мають вразливості на фізичному, канальному та мережному рівнях стеку протоколів передавання.

На фізичному рівні порушник прагне НСД до інформаційної сфери, як правило, шляхом встановлення спеціалізованого обладнання в канали доступу або в магістральні канали. Можливий НСД через консолі управління або активізацією “закладок”, впроваджених в об’єктах цифрових систем передавання. Закладки можуть бути активізовані за допомогою радіоканалів. Після одержання НСД на фізичному рівні атака порушника може розвиватись на канальному і мережному рівнях стека протоколів.

На канальному рівні порушник може виконувати дії на активізацію вразливості відповідних протоколів. Порушник може одержати доступ до інформації, активізувати “закладку” формуванням спеціальних команд в кадрах (комірках, контейнерах) даних. Команди можуть розміщуватись в заголовку, в полі даних, в полі контрольної суми. Небезпечні атаки блокування передавання повідомлень, що можуть бути реалізовані несанкціонованим формуванням прикмет перевантаження, та які викликають масові повтори передачі.

На мережному рівні активізуються вразливості протоколів цього рівня. Порушник може отримати НСД до інформації і провести атаки типу блокування передавання, блокування доступу тощо.

2.3 Загальні положення безпеки інформаційних ресурсів у програмно-керованих АТС

2.3.1 Вимоги до забезпечення інформаційної безпеки програмно-керованої ЦАТС як складової частини телекомунікаційних мереж

Згідно Закону “Про телекомунікації” в ЦАТС та телекомунікаційних мережах, повинна бути забезпечена інформаційна безпека телекомунікаційних мереж, тобто здатність телекомунікаційних мереж забезпечувати захист від:

- знищення інформації;
- перекручення інформації;
- блокування інформації;
- несанкціонованого витоку інформації;
- порушення встановленого порядку маршрутизації інформації.

Необхідною умовою для забезпечення інформаційної безпеки є:

- реалізація сталості телекомунікаційної мережі, тобто властивості телекомунікаційної мережі зберігати повністю, або частково, свої функції за умови впливу на неї дестабілізуючих чинників;

- реалізація забезпечення надійності телекомунікаційних мереж;

- захист інформації сигналізації, синхронізації та управління вузлами доступу, вузлами комутації, вузлами надання послуг та телекомунікаційною мережею в цілому, яка містить важливі для підприємства відомості, порушення цілісності, доступності та конфіденційності яких може привести до моральних чи матеріальних збитків.

Реалізація необхідних умов інформаційної безпеки має проводитись з урахуванням їх технологічних особливостей на основі єдиних стандартів, норм та правил, оскільки в інформаційно-телекомунікаційній мережі мають бути визначені ролі суб'єктів служби захисту.

Згідно Законів України "Про основи національної безпеки України", "Про телекомунікації", "Ліцензійних умов проводження діяльності у сфері телекомунікацій …" та інших нормативно-правових документів оператор у сфері діяльності з питань, пов'язаних з формуванням, використанням та захистом національних ресурсів має забезпечити інформаційну безпеку в таких напрямках:

- установлювати спеціальний режим доступу відповідно до законодавства на об'єктах телекомунікацій, а також в окремих структурних підрозділах, де передається, обробляється або зберігається **інформація з обмеженим доступом, що є власністю держави**;

- вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, **інформації з обмеженим доступом про організацію й функціонування телекомунікаційних мереж та інформації, що передається цими мережами** в інтересах задоволення потреб національної безпеки, оборони та охорони правопорядку;

- забезпечувати **готовність телекомунікаційних мереж зв'язку до роботи в умовах надзвичайних ситуацій, надзвичайного та воєнного стану**, у тому числі можливість оповіщення своїх споживачів у цих умовах, взаємодіючи при цьому з національним центром оперативно-технічного управління мережам телекомунікацій України в питаннях, віднесених до компетенції оператора;

- встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення відповідно до діючого законодавства. Оператор телекомунікацій зобов'язаний забезпечувати **захист зазначених технічних засобів від несанкціонованого доступу**;

- задовольняти вимоги споживачів щодо **збереження конфіденційності інформації, яка стосується споживача**, забезпечувати та нести відповідальність за схоронність відомостей щодо споживача, отриманих при

укладенні договору, наданих телекомунікаційних послуг, у тому числі номенклатури отримання послуг, їх тривалості, змісту, оплати, маршрутів передавання тощо. Зокрема, під час автоматизованої обробки інформації про абонентів необхідно забезпечувати її захист відповідно до закону;

- забезпечувати під час замовлення та/або надання телекомунікаційних послуг фіксованого телефонного зв'язку **безпеку телекомунікаційних послуг** та надавати споживачам послуги за встановленими показниками якості та захищеності телекомунікаційних послуг;

- забезпечити **таємницю зв'язку** згідно із законодавством, охорону таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передається технічними засобами телекомунікацій, та **інформаційну безпеку телекомунікаційних мереж**;

- додержуватися встановленого нормативно-правовими актами **порядку маршрутизації трафіка,** забезпечити резервування технічних засобів телекомунікацій, фрагментів телекомунікаційних мереж і альтернативні маршрути в разі пошкодження при надзвичайних ситуаціях у телекомунікаційній мережі загального користування;

- вживати заходів для недопущення **несанкціонованого доступу до телекомунікаційних мереж та інформації**, що передається цими мережами. Зняття інформації з телекомунікаційних мереж заборонено, крім випадків, передбачених законом.

Заходи та засоби захисту телекомунікаційних мереж та інформації, що циркулює ними, мають застосовуватись на всіх, без винятку, етапах їх життєвого циклу:

- розробки технічного завдання чи технічних умов на створення, техніко-робочого проектування, будівництва, здавання до експлуатації, власне експлуатації, виведення з експлуатації та утилізації;

- на етапах погодження засобів телекомунікацій, які можуть застосовуватися в телекомунікаційних мережах. Одними з критеріїв прийняття рішень є забезпечення надійності та безпеки мереж телекомунікацій. Розвиток та вдосконалення телекомунікаційних мереж має проводитись з урахуванням технологічної цілісності всіх мереж та їх інформаційної безпеки. Договори на постачання телекомунікаційних засобів та обладнання мають включати в себе вимоги щодо інформаційної безпеки ЦАТС;

- етапи будівництва, реконструкції й модернізації телекомунікаційних мереж не повинні призводити до зниження надійності та рівня захищеності ЦАТС. Проекти будівництва, реконструкції та модернізації телекомунікаційних мереж, і в тому числі проекти комплексних систем захисту інформації, підлягають експертизі в порядку, встановленому законодавством;

- на етапі технічної експлуатації телекомунікаційних мереж оператором телекомунікацій ця діяльність повинна здійснюватись тільки за умови наявності проектної документації, розробленої у відповідності до норм технологічного проектування та вимог керівних нормативних документів, зокрема вимог нормативних документів сфери технічного захисту інформації (ТЗІ). Технічне обслуговування технічних засобів телекомунікацій та каналів

електрозв'язку повинне забезпечуватись у відповідності до нормативних та технічних документів, чинних у сфері телекомунікацій і, зокрема, нормативних документів сфери ТЗІ.

Обов'язковий ТЗІ, спрямовано на забезпечення конфіденційності, цілісності та доступності інформації, яка циркулює в телекомунікаційній мережі та її системі управління, здійснюється згідно законодавства України.

Згідно законодавства України в телекомунікаційних мережах загального користування, які надаються системі урядового зв'язку, національній системі конфіденційного зв'язку, органам з надзвичайних ситуацій, безпеки, оборони, внутрішніх справ України в інтересах задоволення потреб національної безпеки, оборони, охорони правопорядку, обов'язковий ТЗІ спрямовано на забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в телекомунікаційній мережі та її системах управління.

Щодо порядку захисту державних інформаційних ресурсів, тобто інформації, яка є власністю держави та (або) необхідність захисту якої визначено законодавством, діють положення нормативно-правових документів:

- в автоматизованих системах повинен забезпечуватися захист від несанкціонованого доступу (НСД) до державних інформаційних ресурсів з боку будь-яких мереж передачі даних;
- конфіденційність інформації, яка є державними інформаційними ресурсами, під час передавання мережею передачі даних забезпечує власник автоматизованої системи або оператор мережі передачі даних за договором із власником автоматизованої системи;
- захист державних інформаційних ресурсів у мережі передачі даних повинен забезпечуватися впровадженням на кожному з її вузлів комутації комплексу технічних, криптографічних, організаційних та інших заходів і засобів захисту інформації, спрямованих на недопущення її блокування та/або модифікації;
- розроблення, виробництво, впровадження та обслуговування комплексної системи захисту інформації (КСЗІ) здійснюється оператором мережі передачі даних самостійно за умови наявності у нього ліцензії на проведення відповідних видів робіт, або сторонньою організацією, яка має ліцензію на проведення даних видів робіт;
- передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності КСЗІ вимогам із захисту інформації згідно нормативних документів з ТЗІ;
- під час підключення до глобальних мереж абоненти повинні дотримуватися вимог законодавства щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

Система інформаційної безпеки повинна впорядкувати контроль за критичною, з точки зору підприємства, інформацією, застосуванням нових технологій, попередженням подій, що можуть привести до порушення працездатності телекомунікаційних систем або до збитків внаслідок порушення інформаційної безпеки.

2.3.2 Мета та принципи діяльності щодо забезпечення інформаційної безпеки ЦАТС

Головною метою системи інформаційної безпеки є забезпечення стійкого функціонування ЦАТС та мережі зв'язку, попередження загроз їх безпеці, захист законних інтересів підприємства від протиправних посягань, недопущення крадіжки фінансових засобів, розголошення, утрати, спотворення та знищення службової (та управлінської) інформації, забезпечення нормальної виробничої діяльності усіх підрозділів об'єкта.

Крім того, метою системи інформаційної безпеки є підвищення якості наданих послуг та гарантії безпеки майнових прав та інтересів абонентів. У технічному плані мета захисту ЦАТС полягає у виконанні норм, заходів та дій, спрямованих на запобігання шкоди і/або збитків у разі реалізації атаки на інформаційну безпеку.

Захист здійснюється КСЗІ, яка складається з правового, організаційно-методичного, технічного, програмного, інформаційного та математичного забезпечень, що запобігають або суттєво утруднюють реалізацію атак.

Центри комутації та їх виноси розташовані на невеликих територіях і захищаються методом "кругової оборони" (бар'єрним методом).

Лінії зв'язку, магістралі проходять незахищеною територією і захищаються шляхом розподілу механізмів захисту по їх елементам або "компенсаційним" методом, шляхом встановлення відповідних засобів захисту в центрах та прикінцевому обладнанні.

Станційне обладнання ЦАТС розміщується на охороняємому об'єкті, де проводиться повний цикл організаційно-технічних заходів з комплексної інформаційної безпеки певного атестованого рівня.

Обладнання програмно-керуємих АТС та іншого обладнання ЦАТС має штатну систему захисту інформаційної безпеки, здатну забезпечувати захищеність рівня, який забезпечується фірмою-виробником даного обладнання згідно договору на постачання.

Телекомунікаційні мережі захищаються «розподіленим методом». Кожна з технологічних мереж повинна мати свою власну КСЗІ, побудовану на основі політики захисту інформаційних ресурсів в даній мережі, інтерфейси яких мають бути узгодженими з КСЗІ розглянутої ЦАТС.

Кожна ЦАТС повинна мати КСЗІ, побудовану на основі політики захисту інформаційних ресурсів для відповідного ЦАТС.

Основними принципами діяльності щодо інформаційної безпеки є такі:

- забезпечення прав громадян, суспільства та держави на використання інформаційних технологій із забезпеченням визначеного рівня захищеності інформації;
- легітимності – ТЗІ повинен здійснюватись згідно з вимогами чинних в Україні нормативно-правових актів та нормативних документів щодо ТЗІ;
- комплексності – ТЗІ має здійснюватись комплексом взаємопов'язаних організаційних і інженерно-технічних заходів;
- мінімальної достатності – необхідний рівень захищеності повинен досягатись при мінімальних витратах;

- адаптивності – в залежності від конкретних вимог національної безпеки мають здійснюватись зміни пріоритетів в діяльності щодо ТЗІ та відповідні зміни стратегій забезпечення безпеки;

- безперервності – заходи щодо ТЗІ здійснюються на всіх технологічних етапах надання послуг зв'язку;

- сумісності та безконфліктності засобів захисту;

- систематичності – постійний аналіз загроз, що мають суттєве значення для користувачів та відповідне попереджуюче впровадження засобів протидії цим загрозам в тій мірі, за якої витрати на протидію загрозам не перевищують збитків від їх здійснення;

- збереження якісних показників – технічні та програмні засоби, що використовуються для забезпечення ТЗІ, не повинні суттєво погіршувати основні технічні показники засобів та систем зв'язку;

- контрольованості - наявність можливості моніторингу ефективності заходів щодо ТЗІ;

- керованості в залежності від вимог до захищеності інформації та мінімізації витрат. Має створюватись система управління комплексами засобів захисту, що дозволяє здійснити безперервний контроль ефективності засобів захисту та підтримку необхідного рівня захищеності інформаційних ресурсів ЦАТС;

- масштабованості – можливість легкого нарощування КСЗІ одночасно з розширенням ємності ЦАТС;

- адекватності заходів захисту інформації реальним та потенційним загрозам.

Загальним принципом діяльності в сфері інформаційної безпеки є максимум ефективності за допустимого ризику не нижчого від зафіксованого, коли оперативний ризик є мінімальним.

КСЗІ реалізують як сукупність функціональних послуг захисту (ФПЗ). Послуги захисту та механізми, що їх реалізують, поділяються на штатні і додаткові (позаштатні). У сукупності зі штатними додаткові механізми повинні забезпечити зазначений у технічному завданні рівень захищеності інформації.

На етапі проектування виконується оцінка реалізованих у ЦАТС штатних ФПЗ на відповідність наведеній у технічному проекті моделі захисту. Відсутні послуги реалізуються за допомогою додаткових засобів і механізмів захисту.

Додаткові засоби розробляються, якщо рівень захищеності та рівень гарантій захищеності недостатній. КСЗІ ЦАТС повинна реалізувати такі функції захисту інформації.

Загальні послуги безпеки повинні надаватись незалежно від складу і функціональних можливостей ЦАТС на протязі всього їх життєвого циклу. Ці послуги повинні бути узгоджені у всіх взаємодіях підсистем, об'єктів і суб'єктів ЦАТС. До складу загальних послуг безпеки ЦАТС мають входити:

- послуги ідентифікації та аутентифікації;

- послуга управління доступом, що повинна специфікувати множину припустимих для кожного суб'єкта операцій з кожним об'єктом і постійний контроль додержання цих специфікацій;

- послуга цілісності, що повинна забезпечити повноту, точність та достовірність інформації;

- послуга конфіденційності, що повинна забезпечити недоступність та нерозкриття інформації ЦАТС користувачам, що не мають для цього необхідних повноважень;

- послуга доступності.

Послуги безпеки ЦАТС реалізуються за допомогою штатних та додаткових механізмів безпеки. Рівень захисту, який визначено політикою безпеки ЦАТС, досягається вибором механізмів безпеки відповідного класу, що можуть перетинатись.

Закон вимагає застосовувати в телекомунікаційних мережах лише такі засоби телекомунікацій, які мають підтвердження відповідності чинним нормативним документам у сфері телекомунікацій та технічним регламентам, критеріям забезпечення надійності, безпеки мереж телекомунікацій.

2.3.3 Пріоритети забезпечення інформаційної безпеки ЦАТС

Пріоритети ранжуються у залежності від важливості інформації та мінімізації збитків відповідно за напрямами забезпечення інформаційної безпеки, а також найменш прорублені в силу ситуації з інформаційною безпекою, що склалася:

- зважаючи, що згідно нормативно-правових документів *передавання державних інформаційних ресурсів дозволяється лише через вузли комутації, що мають атестат відповідності КСЗІ вимогам із захисту інформації, який надається за результатами державної експертизи в сфері технічного захисту інформації,* пріоритетним є проведення робіт по розгортанню КСЗІ на ЦАТС та їх атестація;

- для забезпечення керованості системи інформаційної безпеки, в залежності від вимог до захищеності інформації та мінімізації витрат, має створюватись *система управління інформаційною безпекою* та комплексами засобів захисту, що дозволить здійснити необхідний безперервний контроль ефективності засобів захисту, підтримку необхідного рівня захищеності інформаційних ресурсів ЦАТС, визначення механізму оцінки ступеню важливості інформації, розмірів ймовірної шкоди у разі несанкціонованого доступу до інформаційних ресурсів, порядку оцінки та витрат, пов’язаних з проведенням робіт із забезпечення вимог інформаційної безпеки;

- в галузі зв’язку має активізуватись створення систем захисту від несанкціонованого використання ресурсів систем телекомунікацій, розгортання систем запобігання несанкціонованому доступу, боротьби із шахрайством і моніторингу якості та рівня інформаційної безпеки мереж;

- створити та ефективно використовувати оптимізовані профілі захисту, адаптовані до конкретних підприємств на основі апробованих та адаптованих методик оцінки інформаційної безпеки;

- виробити та обґрунтувати необхідні організаційні заходи: склад і структуру служби інформаційної безпеки, пакет посадових інструкцій, інструкції дій в нештатних ситуаціях, обґрунтувати необхідні вкладення в захист інформації, обґрунтовано вибрати апаратно-програмні засоби захисту інформації у рамках єдиної концепції безпеки.

- запровадити систему управління інформаційною безпекою у всіх підрозділах підприємства.

Характерним є збільшення пріоритету захисту відкритої інформації. Так, КСЗІ вузла доступу до Інтернет має забезпечувати реалізацію вимог із захисту цілісності та доступності розміщеної на *WEB*-сторінці загальнодоступної інформації, а також конфіденційності та цілісності технологічної інформації *WEB*-сторінки.

Слід запропонувати плани захисту конфіденційної та відкритої інформації, яка передається мережами загального користування, захисту інформації від зловмисного спотворення чи знищення, від НСД до неї, її копіювання або несанкціонованого використання.

2.4 Загальні напрями діяльності щодо забезпечення інформаційної безпеки ЦАТС

2.4.1 Головні завдання діяльності в сфері ТЗІ

Головні завдання щодо організаційного, нормативно-правового забезпечення діяльності в сфері ТЗІ, які для ЦАТС конкретизуються таким чином:

- розвиток і удосконалення системи ТЗІ;
- впровадження заходів щодо мінімізації можливості впливу загроз інформації, що передається, обробляється та зберігається в телекомунікаційних мережах;
- визначення механізму оцінки ступеню важливості інформації, розмірів ймовірної шкоди у разі несанкціонованого доступу до інформації з обмеженим доступом, порядку оцінки та витрат, пов’язаних з проведенням робіт із забезпечення вимог ТЗІ;
- визначення порядку розрахунку збитків, які можуть бути завдані користувачу або постачальнику послуг зв’язку в результаті реалізації загроз для інформації з урахуванням категорії відомостей;
- сертифікація засобів зв’язку на відповідність вимогам захищеності від витоку інформації;
- атестація систем та засобів технічного захисту інформації в умовах конкретного застосування;
- забезпечення державного нагляду та контролю за дотриманням правил використання засобів зв’язку;
- ведення моніторингу рівня захисту інформації та блокування несанкціонованого доступу до неї і планування адекватних заходів реагування на інциденти з безпекою;
- ведення моніторингу нових подій, пов’язаних із законодавчо-нормативними організаційними і технічними аспектами захисту інформації й несанкціонованого доступу до неї, та підготовка своєчасних пропозицій щодо впровадження передового світового досвіду;
- організація підготовки та перепідготовки з питань ТЗІ фахівців зв'язку та осіб, відповідальних за ТЗІ;

Під час створення нормативно-методичної бази ТЗІ галузі та підприємства слід здійснити: визначення основних напрямків стандартизації в сфері ТЗІ і її пріоритетів; збір, систематизацію та аналіз відомостей щодо стану вітчизняної та зарубіжної нормативно-правової бази в сфері ТЗІ; створення нормативних документів з питань ТЗІ, гармонізованих з міжнародними рекомендаціями та стандартами. Мають бути розроблені:

а) система критеріїв оцінювання захищеності інформації для кожного з елементів та ЦАТС в цілому;

б) типові методики оцінки ефективності захисту відповідно до розроблених критеріїв для кожного з елементів та ЦАТС в цілому;

в) методики визначення вимог до нормованих рівнів захищеності інформації та рівнів довіри до коректності реалізації захисту;

г) галузеві нормативні документи щодо порядку ведення робіт з ТЗІ, порядку оцінювання захищеності, сертифікації, атестації тощо;

Необхідно розробити нормативні, методичні і технічні документи з інформаційної безпеки ЦАТС та їх елементів – каналів управління, сигналізації, синхронізації, систем комутації, систем передачі. У складі цих документів повинні бути моделі загроз, профілі захисту, плани захисту, управління рівнем захищеності тощо.

2.4.2 Головні напрями діяльності із забезпечення інформаційної безпеки ЦАТС

Головними напрямами діяльності із забезпечення інформаційної безпеки в ЦАТС є:

- планування діяльності у сфері інформаційної безпеки та прогнозування термінів реалізації запланованих заходів;
- розроблення практичних підходів до реалізації системи інформаційної безпеки в ЦАТС в частині організаційних, правових, технічних, програмних, економічних, соціальних аспектів;
- обґрунтування доцільності створення, структури і завдань підрозділів інформаційної безпеки ЦАТС, які мають безпосередньо забезпечувати виконання всього комплексу завдань захисту мереж телекомунікації та інформації;
- встановлення категорій споживачів за пріоритетами інформації, що захищається, номенклатурою та рівнями якості послуг;
- розроблення принципів та засобів реалізації системи забезпечення захисту інформації на засадах нормативних документів системи ТЗІ на програмно-керованих АТС загального користування, галузевих КНД стосовно інформаційної безпеки в ЦАТС, мережах передачі, системі управління, міжнародних стандартів щодо проектування та управління інформаційною безпекою [16];
- розроблення принципів та засобів управління інформаційною безпекою в ЦАТС; забезпечити впровадження, експлуатацію та контроль функціонування засобів забезпечення інформаційної безпеки, в тому числі:
  - контролю цілісності переданих повідомлень і голосу в умовах реалізації загроз;

- захисту від активізації порушником закладок, впроваджених у інформаційну сферу ЦАТС;
- забезпечення конфіденційності інформації управління, тарифікації, персональних даних тощо; захист від порушення працездатності ЦАТС;
- розроблення нормативно-методичних документів із захисту інформації в мережі синхронізації вузлів зв'язку і мережі сигналізації SS 7.

Ряд аспектів забезпечення інформаційної безпеки ЦАТС мають вирішуватись на рівні усього підприємства. Зокрема це такі аспекти.

Забезпечення єдності економічних, технічних та організаційних методів, оцінних критеріїв та засобів визначення достовірності оцінки рівня інформаційної безпеки для підвищення ефективності діяльності підприємства.

Формування єдиних політики та концепції безпеки об'єктів підприємства, методик розрахунку та обґрунтування необхідних витрат на захист підрозділів підприємства.

Організація роботи зі створення та затвердження нормативно-методичної документації в сфері інформаційної безпеки, організація роботи з розробки методів, засобів інформаційної підтримки прийняття рішень в екстремальних ситуаціях та інцидентах з інформаційною безпекою, аналізу способів вирішення проблем, оцінювання та узагальнення отримуваної інформації, терміновому реагуванню на швидкі зміни в ситуації.

Прогнозування та планування розвитку інформаційної безпеки в ЦАТС.

Планування заходів інформаційної безпеки з врахуванням напрямків розвитку інформаційно-телекомунікаційних технологій.

Взаємодія з питань інформаційної безпеки з проектувальниками, виробниками та постачальниками обладнання ЦАТС з метою забезпечення проектування, управління та контролю КСЗІ на всіх етапах життєвого циклу ЦАТС.

Пошук і впровадження методів побудови надійних систем захисту ЦАТС з мінімальними витратами на них.

Вирішити стратегічні питання зі створення підсистеми управління інформаційною безпекою ЦАТС.

Розробити методику аналізу ризиків на основі якісних та кількісних оцінок ризиків.

Розробити порядок та методики інструментального та експертного дослідження елементів інфраструктури ЦАТС на наявність вразливостей.

2.4.3 Атестація комплексної системи захисту інформації в ЦАТС.

Атестація системи інформаційної безпеки елементів і ЦАТС в цілому повинна підтверджуватись проектною документацією, документами щодо вводу в експлуатацію обладнання ЦАТС, сертифікатами на обладнання і проведеними експертизами, у тому числі й програмного забезпечення, аналізом і оцінкою можливостей порушників щодо реалізації загроз інформаційній безпеці, аналізом інформаційної захищеності елементів і ЦАТС у цілому.

Атестація проводиться у відповідності з вимогами нормативних документів системи ТЗІ програмно-керованих АТС та інших. Розробляється порядок,

задачі, цілі та методика атестації інформаційної безпеки ЦАТС на відповідність реалізованому профілю захисту, політиці безпеки та заявленому рівню інформаційної безпеки. При цьому доцільно розробити практичні підходи, прийоми, методику адекватності оцінки досягнутої захищеності, міри гарантії безпеки інформаційного середовища ЦАТС, що базується на оцінках, з якими можна довіряти інформаційному середовищу ЦАТС.

Паралельно розробляються правила та методологія періодичної перевірки відповідності існуючого режиму інформаційної безпеки політиці безпеки, атестації ЦАТС на відповідність вимогам стандарту безпеки; проведення атестаційних перевірок на всіх етапах життєвого циклу системи інформаційної безпеки з метою оцінки поточного рівня безпеки, планування діяльності в сфері інформаційної безпеки.

2.4.4 Управління системою інформаційної безпеки та економічні аспекти

Доцільно розробити методи і засоби інформаційної підтримки та пошуку рішень в екстремальних ситуаціях та інцидентах з інформаційною безпекою:

- кваліфіковане уточнення, класифікація, початковий аналіз інформації щодо екстремальної ситуації;
- вивчення потенційних джерел виникнення екстремальних ситуацій;
- дослідження основних наслідків екстремальної ситуації та ризиків альтернатив прийняття рішень з ліквідації наслідків;
- отримання достовірної інформації керівництвом та операторами у повному обсязі, необхідному і достатньому для стратегічно правильного прийняття рішень;
- аналіз, пошук способів вирішення виникаючих проблем;
- визначення потреб у ресурсах, необхідних для ліквідації наслідків інцидентів з інформаційною безпекою.

Важливим у цьому напрямі є розробка методик прогнозування потреб у ресурсах, необхідних для ліквідації наслідків інцидентів з інформаційною безпекою, моделювання та прогнозування розвитку екстремальних ситуацій.

У напрямі економічних аспектів належить розробити стратегію мінімізації втрат та впливів реалізації загроз інформаційній безпеці на результати діяльності оператора, встановити взаємозв’язок та взаємозалежність між головним критерієм економічної ефективності ЦАТС – доходами, критеріями якості послуг – вартість, швидкість, готовність та критеріями інформаційної безпеки.

Інформаційна безпека від можливих загроз порушників має плануватись для всіх етапів життєвого циклу починаючи від проектних робіт, будівництва, вводу в експлуатацію і впровадження, експлуатації ЦАТС, її утилізації.

2.4.5 Розробка та впровадження комплексу засобів захисту (КЗЗ) від несанкціонованого доступу (НСД).

Засоби з впровадження КЗЗ слід розділити на первинні та основні. Основні засоби є обов’язковими, якщо КСЗІ ЦАТС планується атестувати на

відповідність вимогам нормативним документам України у сфері ТЗІ. *Первинні* засоби впроваджуються на кожній ЦАТС. У їхній склад входять:

- система захисту інформації автоматизованих робочих місць. Ця система має попереджувати НСД з робочих місць операторів. Рекомендується використовувати програмні чи апаратно-програмні комплекси захисту, котрі пройшли сертифікацію на відповідність вимогам з ТЗІ. Має бути обрано автономний чи мережний варіанти комплексу захисту;
- засоби дублювання, резервування, реагування, які схемно-реалізовані у комутаційній системі. Вони призначені для забезпечення необхідної надійності комутаційної системи, зниження ймовірності виникнення загрозливих ситуацій до припустимого рівня;
- контроль сигналізації відкриття обладнання ЦАТС, який призначено для контролю фізичного доступу до вузлів обладнання, а також інформаційних магістралей;
- комплект документації з описання комплексу засобів захисту та інтерфейсів захисту. До складу документації входять:
  - описання принципів побудови та функціонування КЗЗ;
  - модель захисту;
  - описання механізмів захисту тощо;
- керівництво адміністратора безпеки ЦАТС стосовно комплексу засобів захисту. Керівництво повинне мати опис контрольованих функцій, інструкцію щодо регенерації програмного забезпечення, описання старту, тестування, відновлення КЗЗ та роботи із засобами реєстрації.

Основні заходи впровадження комплексу засобів захисту від НСД мають проводитись на всіх етапах життєвого циклу системи інформаційної безпеки. Має бути встановлено порядок проектування засобів захисту інформації, який передбачає на кожному етапі життєвого циклу формування цілей та прийняття рішень щодо інформаційної безпеки. Мають здійснюватись аналіз суб'єктів доступу та їхні потенційні можливості щодо здійснення НСД, розроблення сценаріїв впливу на ПЗ, якщо у ньому існують закладки.

На кожному етапі проводиться оцінювання безпеки системи, супроводжуване гарантіями, які базуються на формальних чи неформальних доведеннях достатності функцій безпеки.

Послідовність робіт із впровадження комплексу заходів й засобів захисту така:

- обстеження ЦАТС і мережі зв'язку;
- розробка стратегії захисту ЦАТС;
- вибір методів та обладнання захисту;
- розробка методики оцінки ефективності захисту;
- обґрунтування інвестицій в інформаційну безпеку – розрахунок економічного ефекту в результаті пропонованих заходів;
- розробка нормативно-методичних документів (профілів захисту, політики безпеки, планів захисту та комплекту інструкцій персоналу);
- створення центра управління інформаційною безпекою (центра реагування).

Впровадження системи безпеки ЦАТС і мережі може виконуватись поетапно, спочатку по “м’якому”, а потім “жорсткому” сценаріям. При “м’якому” сценарію будується захист мережі у точках спряження її з іншими мережами, вважаючи, що загрози мережі виходять ззовні, власні засоби є дружніми.

При “жорсткому” сценарію загроза може виходити з усіх напрямків, у тому числі і від внутрішніх елементів мережі. Захисна оболонка може бути прорвана і атака може бути проведена на вузли, що не мають точок спряження із зовнішніми мережами.

При розробленні та модифікації програмного забезпечення необхідно дотримуватись правил безпеки:

- розроблення процедури модифікації коду, що передбачає обов’язкове тестування кожної версії програмного забезпечення;
- супроводження початкового коду на сервері та захищене пересилання лише об’єктного коду;
- ідентифікація резервних копій тощо;
- надання рекомендацій щодо усунення наслідків при реалізації програмного закладення та стратегії захисту при активації таких закладень.

Важливою частиною роботи з впровадження КСЗІ ЦАТС є розробка методик, інструкцій та настанов роботи з аналізу ризиків інформаційної безпеки, проектуванню та супроводженню системи інформаційної безпеки, які повинні дозволяти:

- проводити кількісну оцінку поточного рівня безпеки, задавати допустимі рівні ризику, розробляти план заходів із забезпечення необхідного рівня безпеки на організаційно-управлінському, технологічному та технічному рівнях;
- розраховувати та економічно обґрунтовувати розмір необхідних вкладень у забезпечення безпеки на основі аналізу ризиків, порівнювати витрати на забезпечення інформаційної безпеки з потенційними збитками та ймовірністю їх виникнення;
- виявляти та проводити блокування найбільш небезпечних вразливостей до здійснення атак на вразливі інформаційні ресурси;
- визначати функціональні відносини та зони відповідальності при взаємодії підрозділів та осіб із забезпечення інформаційної безпеки;
- створювати пакет організаційно-розпорядчої документації з інформаційної безпеки;
- розроблювати та узгоджувати проект впровадження комплексів захисту з урахуванням розвитку інформаційних технологій;
- забезпечувати підтримку та супроводження впровадженого комплексу захисту в змінюваних умовах роботи підрозділу.

Методично-інструктивна частина роботи має завершитись розробкою правил та методології періодичної перевірки відповідності існуючого режиму інформаційної безпеки політиці безпеки, атестації ЦАТС на відповідність вимогам стандарту безпеки; проведення атестаційних перевірок на всіх етапах життєвого циклу системи інформаційної безпеки з метою оцінки поточного рівня безпеки, планування діяльності в сфері інформаційної безпеки.

Важливим є вироблення практичних підходів, прийомів, методики адекватної оцінки фактичної захищеності, міри гарантії безпеки інформаційного середовища ЦАТС, що базується на оцінках, з якими можна довіряти інформаційному середовищу ЦАТС.

Досягнення поставлених задач неможливе без вироблення та обґрунтування необхідних організаційних заходів: складу і структури служби інформаційної безпеки, пакету посадових інструкцій та дій в нештатних ситуаціях, обґрунтування необхідних вкладень в захист інформації, обґрунтованого вибору апаратно-програмних засобів захисту інформації у рамках єдиної стратегії безпеки, організація підготовки та перепідготовки персоналу та фахівців з питань ТЗІ.

Крім того, необхідна розробка деяких науковоємних питань, таких як, методика аналізу ризиків на основі якісних та кількісних оцінок ризиків, порядок та методика інструментального дослідження елементів інфраструктури ЦАТС на наявність вразливостей, методика розрахунку збитків, які можуть бути завдані споживачеві або постачальникові послуг в результаті реалізації загроз тощо.

2.5 Організація та порядок технічного захисту інформації в ЦАТС

Для успішної технічної експлуатації КСЗІ на ЦАТС з досягненням заданого рівня захищеності інформаційних ресурсів та рівня гарантій захисту необхідно правильно організувати заходи з ТЗІ на всіх попередніх етапах створення КСЗІ, зокрема на стадіях побудови та здавання в експлуатацію.

2.5.1 Організація ТЗІ на стадії побудови ЦАТС

Заходи та засоби захисту телекомунікаційних мереж та інформації, що циркулює ними, мають застосовуватись на всіх, без винятку, етапах їх життєвого циклу: розробки технічного завдання чи технічних умов на створення, техніко-робочого проектування, будівництва, здавання до експлуатації, власне експлуатації, виведення з експлуатації та утилізації. При цьому:

- на етапах погодження засобів телекомунікацій, які можуть застосовуватися в телекомунікаційних мережах, одними з критеріїв прийняття рішень є забезпечення надійності та безпеки мереж телекомунікацій;
- розвиток та вдосконалення телекомунікаційних мереж має проводитись з урахуванням технологічної цілісності всіх мереж та їх інформаційної безпеки. Договори на постачання телекомунікаційних засобів та обладнання мають включати в себе вимоги щодо інформаційної безпеки;
- будівництво, реконструкція і модернізація телекомунікаційних мереж не повинні призводити до зниження їх надійності та рівня захищеності. Проекти будівництва, реконструкції, модернізації телекомунікаційних мереж, та проекти комплексних систем захисту інформації підлягають експертизі в порядку, встановленому законодавством. Робоча документація має містити детальні рішення щодо реалізації технічного проекту КСЗІ, щодо забезпечення управління КСЗІ і взаємодії її компонентів, а також документацію, необхідну

для тестування, проведення пусконалагоджувальних робіт, проведення випробувань КСЗІ.

На стадії побудови ЦАТС проводиться обстеження цього об'єкта інформаційної діяльності та створюються документи для побудови КСЗІ об'єкта:

- технічне завдання на проектування КСЗІ об'єкта;
- робочий або технічно-робочий проект на створення КСЗІ об'єкта.

2.5.2 Організація ТЗІ на стадії вводу в експлуатацію ЦАТС

При проведенні робіт із введення в дію та оцінки захищеності інформації в телекомунікаційній системі виконуються роботи, передбачені НД ТЗІ 3.7-003-05 [17], із перевірки КСЗІ на відповідність вимогам нормативних документів з ТЗІ. При підключенні до об'єктів телекомунікаційних мереж та обладнання інших операторів складаються взаємні вимоги до заходів захисту та порядку захисту інформаційних ресурсів у шлюзових точках підключення інших операторів. Взаємні вимоги до інформаційної безпеки телекомунікаційних систем оформляються юридично договорами з іншими операторами у порядку, визначеному законодавством.

2.5.3 Організація ТЗІ на етапі технічної експлуатації ЦАТС

Згідно чинної нормативно-правової бази ТЗІ для організації робіт із створення КСЗІ в ЦАТС (чи для групи ЦАТС) створюється служба захисту інформації та призначаються відповідальні особи.

Організація та забезпечення діяльності в сфері інформаційної безпеки ЦАТС проводиться не відокремлено, а в тісній взаємодії із всіма службами, які мають відношення до технічної експлуатації телекомунікаційних мереж і, зокрема, ЦАТС. Схема взаємодії служб наведена на рис. 2.3. Схемою передбачається функціонування та взаємодія відповідних служб на рівнях Генеральної дирекції, регіональних центрів ТЗІ, філій та безпосередньо в ЦАТС. Розглянемо аспекти організації діяльності, які мають бути сформовані додатково або в складі існуючих.

В системі технічної експлуатації і технічного обслуговування (ТЕ і ТО), поряд з підсистемами забезпечення якості, надійності і сталості мереж, створюється підсистема інформаційної безпеки мереж телекомунікацій та ЦАТС. Підсистема виконує такі функції:

- створює і забезпечує використання систем моніторингу телекомунікацій, ВОЛЗ та центрів мережі для вирішення комплексного контролю телекомунікацій, виявлення несанкціонованого доступу на фізичному рівні, мережному рівні та на рівні надання послуг, локалізації порушень у найкоротші строки;
- створює і підтримує функціонування КСЗІ в ЦАТС у відповідності до державних і галузевих нормативних документів.

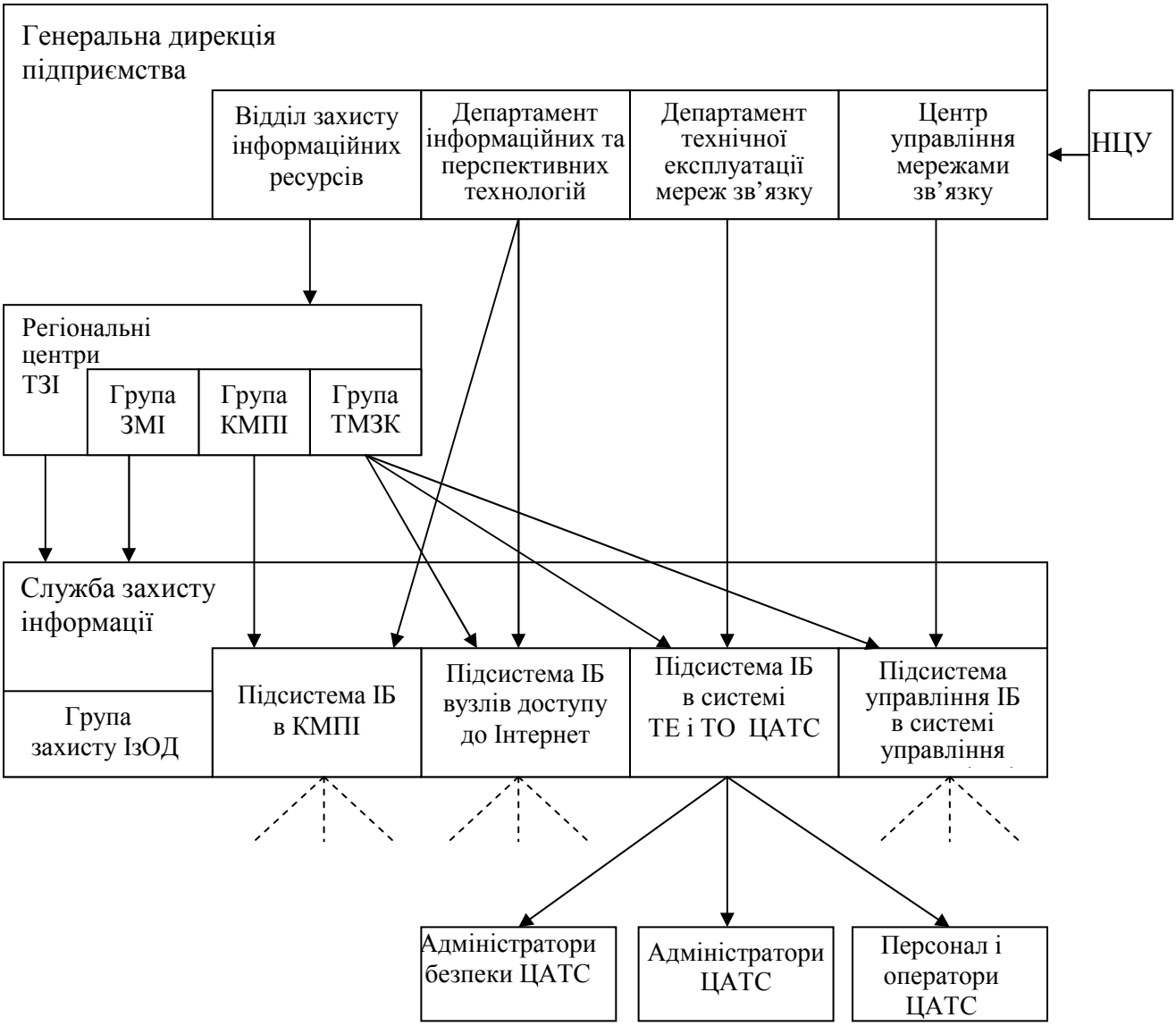

Рисунок 2.3 – Схема організації та забезпечення ТЗІ ЦАТС та мереж

Позначення: ЗМІ – захист мовної інформації; КМПІ – корпоративна мережа передачі інформації; НЦУ – національний центр управління; ІБ – інформаційна безпека; ІзОД – інформація з обмеженим доступом; ТЗІ – технічний захист інформації; ТЕ і ТО – технічна експлуатація і технічне обслуговування; ТМЗК – телекомунікаційна мережа загального користування; ЦАТС – цифрова автоматична телефонна станція.

Група ТЗІ у складі Служби захисту інформації координує і контролює роботи із забезпечення інформаційної безпеки ЦАТС та телекомунікаційних мереж, керує роботою адміністраторів безпеки ЦАТС, надає методичну, інструментальну і технічну допомогу у забезпеченні захисту комерційної таємниці підприємства, готує ЦАТС до державної експертизи та атестації на відповідність вимогам з інформаційної безпеки.

В ЦАТС обов'язки забезпечення інформаційної безпеки на робочих місцях покладаються на всіх, без винятку, працівників в межах означених у їх посадових інструкціях:

- адміністратори безпеки забезпечують функціонування КСЗІ ЦАТС і контролюють стан інформаційної безпеки і роботу адміністраторів мереж і систем та експлуатаційного персоналу. У питаннях інформаційної безпеки адміністратори безпеки підпорядковані і звітують Службі захисту інформації. У технологічних і виробничих питаннях адміністратори безпеки підпорядковані керівництву ЦАТС.

Адміністратори безпеки, в залежності від обсягу роботи, призначаються штатними або суміщають ці обов'язки з іншими обов'язками. Заборонено суміщати функції адміністратора безпеки і адміністратора мережі чи системи, бо це може суттєво знизити рівень інформаційної безпеки ЦАТС;

- адміністратори мереж та систем забезпечують працездатність обладнання ЦАТС та інформаційної безпеки в межах своїх повноважень.

Штатний експлуатаційний персонал додатково до своїх функцій виконує заходи і роботи із підтримання інформаційної безпеки на своїх робочих місцях і в закріпленому за ними обладнанні. Ці функції відмічаються у посадових інструкціях і у окремих інструкціях з інформаційної безпеки.

2.5.4 Організація управління інформаційною безпекою

Для безпосередньої організації роботи із забезпечення інформаційної безпеки (та/або захисту інформації) в структурі управління мережами телекомунікацій має бути створена служба управління інформаційною безпекою, яка повинна забезпечити виконання всього комплексу завдань захисту телекомунікаційних мереж та інформації. Вказаній службі підпорядковуються групи інформаційної безпеки, що створюються на ЦАТС (і/або в структурі місцевої телефонної мережі загального користування), в задачу яких входить комплексне забезпечення інформаційної безпеки.

Управління інформаційною безпекою проводиться на усіх етапах життєвого циклу: планування, створення й експлуатації системи інформаційної безпеки. На стадії технічної експлуатації системи метою процесу управління інформаційною безпекою є оцінювання ефективності створеної системи захисту інформації й вироблення додаткових уточнюючих вимог для доробляння системи захисту з метою забезпечування її адекватності за зміни умов функціонування: характеристик системи, опрацьовуваної інформації, фізичного середовища, персоналу, призначення системи, політики безпеки тощо. Управління інформаційною безпекою базується на практичних правилах, котрі групуються в такі складові:

1) загальні положення з управління інформаційною безпекою:
   - політика безпеки;
   - організація захисту;
   - класифікація ресурсів та їхній контроль;
2) безпека персоналу, фізична безпека й безпека навколишнього середовища;
3) адміністрування комп'ютерних систем та обчислювальних мереж;
4) управління доступом до систем;
5) розробляння й супроводження інформаційних систем;
6) планування захисту:

- планування безперебійної роботи підприємства;
- виконання вимог.

Завдання управління інформаційною безпекою розв'язуються із застосовуванням засобів контролю. Ключовими є такі засоби контролю:

- документ про політику інформаційної безпеки;
- розподіл обов'язків щодо забезпечування інформаційної безпеки;
- навчання й підготовка персоналу до підтримування режиму інформаційної безпеки;
- повідомлення про випадки порушування захисту чи інциденти в системі безпеки;
- засоби захисту від вірусів;
- процес планування безперебійної роботи підприємства;
- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;
- захист документації підприємства;
- захист даних;
- відповідність політиці безпеки.

Реалізація засобів управління безпекою в інформаційній інфраструктурі не повинна заважати іншій виробничій діяльності. Витрати на систему захисту інформації слід привести у відповідність з цінністю інформації, яка захищається, й інших інформаційних ресурсів, піддаванні ризикові, а також зі збитками, що їх може бути нанесено підприємству через збої в системі захисту. Тому в процесі управління мають оцінюватись ризики порушування безпеки. Для оцінювання ризиків слід:

- визначати й аналізувати потенційні загрози, яким піддаються комп'ютерні системи, та їхні вразливості;
- розглядати збитки, котрі можуть нанести діяльності підприємства серйозне порушування інформаційної безпеки, з урахуванням можливих наслідків порушування конфіденційності, цілісності й доступності інформації;
- розглядати реальну ймовірність такого порушування захисту від суттєвих загроз за наявності засобів контролю.

Оцінка ризику залежить від таких чинників:

- характеру виробничої інформації та систем;
- виробничої мети, для якої інформація використовується;
- середовища, в якому система використовується й скеровується;
- захисту, забезпечуваного існуючими засобами контролю.

Успішне здійснення системи інформаційної безпеки визначається таким:

- забезпечування безпеки має ґрунтуватися на виробничих цілях і вимогах;
- функції управління безпекою має взяти на себе керівництво підприємства;
- оцінювання ризиків порушування безпеки, загроз і слабкостей інформаційних ресурсів та рівня їхньої захищеності має ґрунтуватися на цінності й важливості цих ресурсів;
- ознайомлення з системою безпеки всіх керівників та рядових співробітників підприємства;
- вивчання співробітниками політики та стандартів інформаційної безпеки;

- врахування конкретних інформаційних технологій, функцій підприємства та виробничого чи обчислювального середовища.

Згідно зі схемою маршрутизації викликів необхідно передбачити можливість альтернативного виходу до ТМЗК інших операторів, контролювати правильність маршрутизації трафіка, оперативно інформувати НЦУ, інших операторів телекомунікацій взаємо приєднаних мереж стосовно ситуацій, які призвели або можуть призвести до припинення обслуговування трафіка та про надзвичайні ситуації, у тому числі спричинені аваріями, пожежами тощо, використовувати технічні засоби та обладнання телекомунікацій, у тому числі які призначені для обліку обсягів та проведення розрахунків наданих телекомунікаційних послуг, які мають документ про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій та інформаційної безпеки, дотримуватися технічних вимог та вимог з інформаційної безпеки.

2.5.5 Повноваження та відповідальність суб'єктів взаємовідносин при реалізації задач забезпечення інформаційної безпеки в ЦАТС

Суб'єкти взаємовідносин при реалізації задач інформаційної безпеки в ЦАТС, права та повноваження посадових осіб, відповідальність суб'єктів взаємовідносин і ЦАТС при реалізації задач інформаційної безпеки мають відповідати чинним нормативно-правовим документам.

Функції та порядок роботи "Служби захисту інформації" в підрозділах підприємства слід визначати згідно НД ТЗІ 1.4-001-2000 [18].

Права і обов'язки адміністраторів безпеки визначаються наказом та інструкціями, затвердженими керівником підприємства.

2.6 Приклад комплексної системи захисту інформації ЦАТС типу *EWSD*

Розглянемо практичний приклад комплексної системи захисту інформації (КСЗІ), яка реалізує функціональний клас послуг безпеки базового рівня (*FC*-1). Така КСЗІ базується на штатних засобах захисту інформації й може бути впроваджена у ЦАТС шляхом деякої реорганізації системи технічної експлуатації та додаткових позасистемних засобів захисту.

2.6.1 Основні положення комплексної системи захисту інформації станції

Комплексна система захисту інформації (КСЗІ) створюється згідно пакета НД системи ТЗІ на програмно-керованих АТС загального користування [8…18].

Цифрові комутаційні системи (ЦКС), як правило, оснащуються штатними і, при необхідності, додатковими позаштатними засобами ТЗІ, які при їхньому спільному використанні утворюють *комплекс засобів і механізмів захисту* (КЗМЗ), які забезпечують потрібний рівень захищеності інформаційних ресурсів ЦКС, тобто спроможності системи ТЗІ протистояти впливам загроз.

На стадії проектування замовником розробляється підрозділ технічного завдання на будівництво ЦКС за назвою "Вимоги до ТЗІ у ЦКС", технічний та робочий проекти. На стадії розробки робочого проекту системи ТЗІ у ЦКС

виконавцем розробляється КЗМЗ у ЦКС, як взаємопов'язаний набір засобів і механізмів захисту, що реалізують обрану модель захисту. *Модель захисту* розробляється на стадії технічного проектування як взаємопов'язаний набір функціональних послуг захисту з необхідними рівнями ефективності і стійкості реалізації цих послуг, за яких забезпечується заданий у технічному завданні рівень захищеності інформаційних ресурсів в ЦКС.

Приклад *структури ТЗІ в ЦКС* подано на рис. 2.4, де види забезпечення систем ТЗІ подані з різною глибиною деталізації. На рисунку є такі позначення: ТС – технологічне середовище; ФПЗ – функціональні послуги захисту.

ФПЗ є набором елементарних функцій, виконання яких у середовищі експлуатації ЦКС дозволяє протистояти певній множині загроз для інформації.

Засоби ТЗІ в ЦКС складаються із сукупності фізичних, технічних і програмних підсистем захисту, що функціонують на стадії її експлуатації; системи організаційно-технічних та організаційно-адміністративних заходів; системи ліквідації наслідків реалізованих загроз для інформації на АТС; системи управління засобами ТЗІ. Підсистеми захисту в ЦКС класифікуються за способами здійснення загроз і в сукупності повинні забезпечувати реалізацію на практиці обраної моделі захисту з необхідними гарантіями.

Програмні підсистеми захисту забезпечують реалізацію визначеної номенклатури функціональних послуг захисту. ФПЗ в ЦКС здійснюються за допомогою конкретних засобів і механізмів, що поділяються на штатні та додаткові.

Штатні засоби і механізми захисту інформації здебільшого вже закладені в архітектуру сучасних ЦКС або в систему їхньої технічної експлуатації. Додаткові засоби і механізми захисту розробляються й застосовуються у випадках, коли штатні не забезпечують необхідного рівня захищеності.

Номенклатура штатних ФПЗ складається з функцій захисту:

- від несанкціонованих впливів через штатні засоби доступу;
- від позаштатних впливів через штатні основні або додаткові програмні і/або технічні засоби ЦКС;
- від позаштатних впливів на параметри середовища експлуатації ЦКС;
- від впливів з використанням позаштатних програмними і/або програмно-технічними засобами на програми, дані і процеси в ЦКС, що встановлені в процесі її експлуатації; від впливів закладних пристроїв і програмних закладок;
- від впливів позаштатними технічними і/або програмно-технічними засобами на елементи устаткування в процесі експлуатації ЦКС; від витоків інформації через канали побічних електромагнітних витоків та наводок (ПЕМВН);
- від витоків інформації через канали побічних акусто-електричних перетворень; від якісної недостатності інформаційно вразливих режимів, функцій і послуг, що надаються ЦКС та від збоїв і відмов у роботі ЦКС;
- від загроз у системах збереження інформації на фізичних носіях.

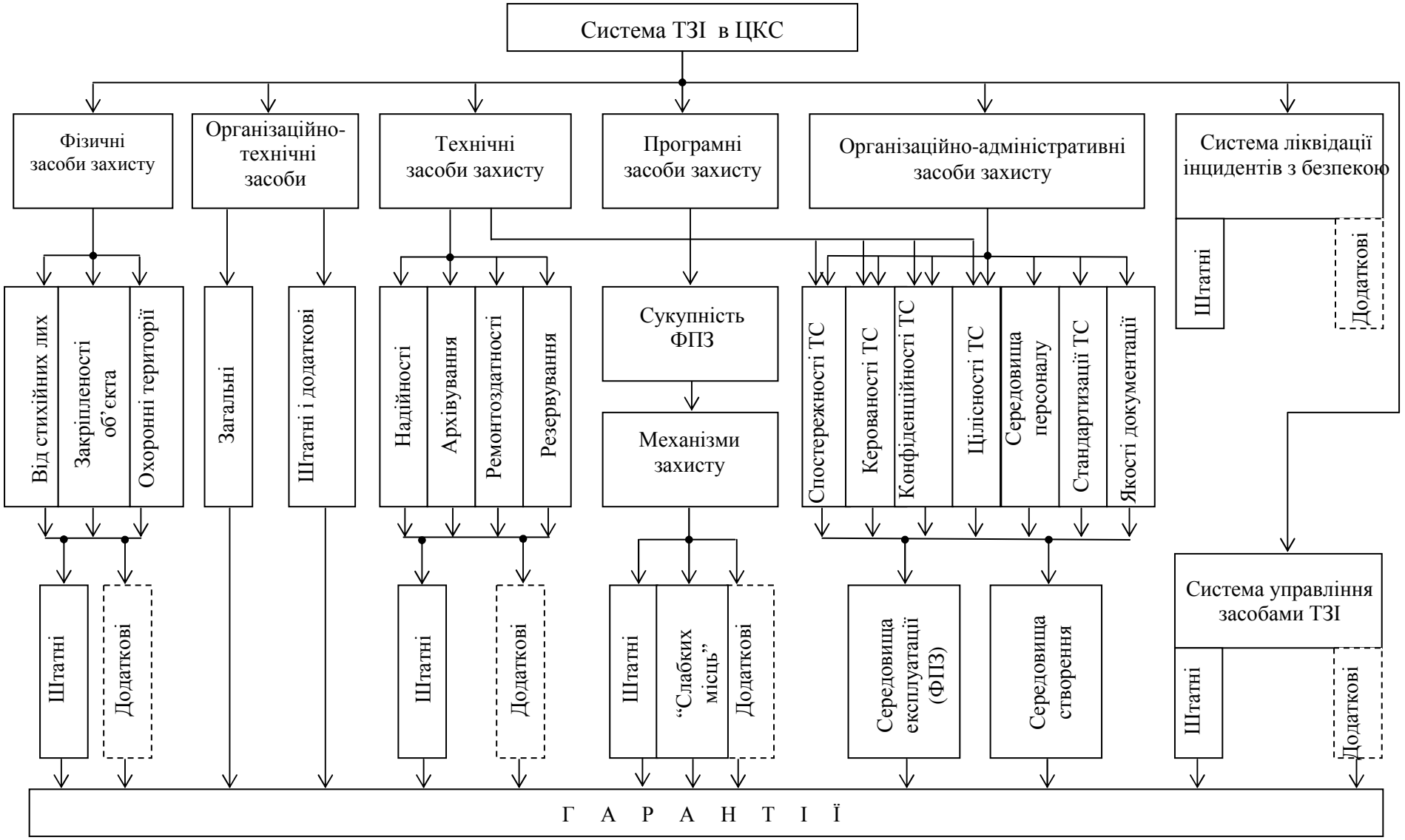

Рисунок 2.4 – Структура забезпечення системи ТЗІ в ЦКС

Крім того, в штатні ФПЗ входять ФПЗ ліквідації наслідків реалізованих загроз для інформації в ЦКС та управління засобами ТЗІ.

Технічні підсистеми захисту включають засоби підтримки надійності, архівування програм та даних, ремонтоздатності та резервування.

Система фізичних заходів захисту включає засоби укріпленості об'єкта, охорони території, засоби захисту від стихійних лих тощо.

Система організаційно-технічних заходів, що здійснюється на всіх стадіях життєвого циклу ЦКС, повинна знизити рівні кількісної і якісної недостатності компонентів і всієї ЦКС у цілому до можливих і/або припустимих значень.

Система ліквідації наслідків реалізованих загроз для інформації, що являє собою сукупність програмно-апаратних засобів і відповідних організаційних заходів, повинна знизити рівень втрат від реалізованих загроз для інформації до можливих і (або) припустимих меж.

Система управління засобами ТЗІ повинна забезпечувати безперервний контроль і підтримку певного рівня захищеності інформації в ЦКС на стадії її експлуатації. Ресурси, що пов'язані з ТЗІ, включаються в об'єкти доступу і, отже, потребують захисту.

Система організаційно-адміністративних заходів разом з іншими системами захисту забезпечують гарантії захисту інформаційних ресурсів технологічних середовищ створення та експлуатації ЦКС. Ці гарантії необхідні для визначення рівнів довіри до коректності розробок, реалізацій та експлуатації систем ТЗІ в ЦКС. Оцінка рівнів довіри виконується відповідно до НД ТЗІ 3.7-002-99.

Система гарантій включає п'ять аспектів забезпечення захищеності інформації в технологічному середовищі створення та експлуатації систем ТЗІ і ЦКС у цілому:

- гарантії безпеки середовища персоналу;
- гарантії стандартизації технологічного середовища;
- гарантії забезпечення спостережності і керованості технологічного середовища;
- гарантії забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища;
- гарантії якості документації.

Кожен аспект деталізується на конкретні вимоги. Так, необхідно виконати низку вимог до безпеки середовища персоналу:

- вимоги до системи організації праці;
- до контролю системи організації праці;
- до поведінки персоналу та контролю поведінки персоналу в робочий та неробочий час.

Для одержання гарантій забезпечення якості стандартизації технологічного середовища необхідно виконати вимоги:

- до повноти охоплення стандартами елементів середовища;
- до глибини охоплення стандартами технологій роботи в середовищі;
- до рівня значимості та взаємоузгодження.

Для забезпечення гарантій якості документації необхідно виконати вимоги: до повноти документації, до рівня деталізації опису середовища і/або технологій, до вірогідності інформації, що міститься в документації та до якості оформлення документації.

Задоволення вимог до спостережності і керованості технологічного середовища та конфіденційності і цілісності інформаційних ресурсів технологічного середовища дозволяє реалізувати обраний функціональний профіль вимог до захищеності інформації в ЦКС.

Відповідно до принципу мінімальної достатності, система захисту повинна бути спроектована таким чином, щоб здійснювалася протидія тільки тим загрозам, що мають суттєве значення для Замовника системи ТЗІ, і тільки в тій мірі, у якій необхідно нейтралізувати чи послабити, зменшити наслідки прояву таких суттєвих загроз, для того щоб втрати від їхніх можливих реалізацій не перевищили гранично припустимих рівнів.

На стадії технічного проектування розробляється модель захисту інформаційних ресурсів ЦКС. Вибір моделі захисту являє собою рішення задачі з мінімізації ресурсів захисту при забезпеченні наведеного в технічному завданні рівня захищеності інформаційних ресурсів ЦКС. У результаті рішення визначається сукупність ФПЗ для реалізації КЗМЗ в системі ТЗІ.

Для вперше створюваних ЦКС спочатку виконується вибір системи з оглядом на реалізовані у ній ФПЗ таким чином, щоб мінімізувати вартість робіт із створення додаткових механізмів захисту, якщо в цьому виникає потреба. У сукупності зі штатними додаткові механізми повинні забезпечити зазначений у технічному завданні рівень захищеності інформації. Необхідно вибрати таку систему, штатні засоби захисту якої найбільш повним чином реалізовували б отриману за результатами технічного проектування модель захисту. Якщо тип ЦКС вже обрано, то виконується оцінка реалізованих у ній штатних ФПЗ на відповідність наведеній у технічному проекті моделі захисту. Відсутні послуги реалізуються за допомогою додаткових засобів і механізмів захисту.

Аналогічно, для штатних організаційно-технічних засобів і заходів (перепускний режим, охорона території, протипожежна сигналізація, кліматика тощо) проводиться оцінка достатності рівня захищеності, які вони забезпечують. Додаткові засоби розробляються, якщо рівень захищеності та рівень гарантій захищеності недостатній.

Для додаткових засобів та механізмів захисту враховується повний життєвий цикл: пошук “слабких місць”, проектування, створення, оцінка або тестування, атестація, супроводження, експлуатація.

2.6.2 Інформація, яка підлягає захисту

Для АТС з програмним управлінням (цифрових) під інформацією абонента розуміється розмова, а також поступово збільшувана частка високоякісних аудіо та відео-повідомлень, тексту, даних та нових інтерактивних послуг.

Крім інформації абонентів в АТС з програмним управлінням циркулює та зберігається технологічна інформація з обмеженим доступом, правила доступу

до якої визначаються чинним законодавством. Вона підлягає захисту і до неї відноситься:

- дані системи технічного обслуговування АТС;
- дані про конфігурацію АТС;
- інформація бази даних, яка забезпечує процес встановлення з'єднань;
- інформація бази даних управління додатковими послугами;
- програмне забезпечення АТС.
- данні управління мережею;

Підлягають захисту на загальних засадах і допоміжні види інформації, оскільки функціональні вузли, до яких вона належить, інтегровані в АТС:

- інформація про категорії абонентів;
- інформація обліку вартості надання послуг зв'язку;
- інформація обліку та контролю телефонного навантаження;
- інформація про якість надання послуг;
- інформація щодо дії персоналу АТС;
- дані про стан апаратної та програмної частини АТС;
- дані щодо міжстанційної сигналізації.

Конфіденційність, цілісність, доступність та керованість інформації абонентів забезпечується шляхом надання послуг зв'язку згідно з нормативними документами галузі зв'язку.

2.6.3 Загрози інформації

КСЗІ має протидіяти загрозам інформаційним ресурсам ЦАТС, у перелік яких входять:

- лавиноподібне зростання кількості телефонних викликів;
- несанкціоноване адміністрацією оператора зв'язку користування з боку "тіньових" абонентів послугами, що надаються ЦАТС *EWSD*;
- несанкціоноване користування іншими операторами зв'язку послугами, що надаються ЦАТС *EWSD* за рахунок порушення цими операторами угод щодо порядку оплати для транзитних ЦКС міжстанційного трафіка;
- несанкціонований доступ (НСД) до наступних програмних елементів ЦАТС *EWSD*:
  - до операційної системи (ОС);
  - до програмного забезпечення користувача;
  - до програмного забезпечення системи технічної експлуатації;
  - до спеціалізованих програм управління з'єднаннями;
- НСД до наступних модулів чи підсистем ЦАТС EWSD:
  - до технологічних баз даних, що розміщені на комутаційних модулях;
  - до системного терміналу або АРМу, що приєднано або може бути приєднано до підсистеми управління;
  - до модемної лінії доступу до модуля технічної експлуатації;
  - до фізичних носіїв інформації із програмним забезпеченням;
  - до станційного кросу;

- активізація закладних пристроїв і (або) програмних закладок, що встановлені в елементах підсистеми управління на передексплуатаційних стадіях життєвого циклу ЦАТС;

- активізація нештатних додаткових видів обслуговування (ДВО).

Загрозам протистоять функціональні послуги захисту (ФПЗ), які являють собою взаємопов'язаний набір виконуваних у середовищі експлуатації ЦАТС елементарних функцій, що дозволяє протистояти певній множині загроз для інформації.

2.6.4 Штатний комплекс засобів та механізмів захисту, реалізований у цифровій комутаційній системі типу *EWSD*

Штатний комплекс засобів та механізмів захисту (КЗМЗ), який реалізовано у цифровій комутаційній системі (ЦКС) типу *EWSD*, складається з функціональних послуг захисту (ФПЗ), кожна з яких протистоїть певній множині загроз. У сукупності це ті ФПЗ, які протистоять тим десяти видам загроз, які наведені в розд. 2.1.3.

ФПЗ, що надаються штатним КЗМЗ, наведені у табл. 2.1. Читач може впевнитись, що наведений комплекс протистоїть усім видам загроз, наведеним у розд. 2.1.3.

Прийнята досить складна *система позначень штатних ФПЗ за допомогою термів* довільної довжини.

Перший символ терму – літера Ф є заголовком терму.

Наступні дві цифри є кодом підсистеми ЦАТС, які наведені на рис. 2.1 і відрізняються за різними технічними каналами витоку, спеціальних впливів та НСД.

Решта символів терму є послідовність змістовних скорочень, що поєднані між собою спеціальними розмежувачами (/), які разом із трьома попередніми символами утворюють у контексті код ФПЗ.

Змістовні скорочення складаються з трьох семантичних частин:

- скорочення для позначення дій (три букви);
- скорочення для позначення місць і (або) предметів розгляду (дві букви);
- скорочення для уточнення дій, місць та предметів розгляду (одна буква).

За деталями скорочень відсилаємо до НД ТЗІ 2.5-001-99 [9].

Наприклад, скорочення Ф01/РДО/Д'Н/АЛ\ПС означає:

Ф – заголовок терму;

01 – підсистема захисту від несанкціонованих впливів суб'єктів доступу через штатні термінали обслуговування і штатні абонентські прикінцеві пристрої;

РДО – розмежування доступу;

Д'Н – довірче та мандатне;

АЛ – абонентська лінія або абонентський прикінцевий пристрій;

ПС – послуга.

Цей код означає – використання змішаної стратегії управління доступом, що застосовується з боку телефонних комутаторів і прикінцевих абонентських

пристроїв до сервісних функцій і послуг ЦКС, що й наведено у першому рядку табл. 2.1.

В результаті реалізації штатних ФПЗ програмними чи апаратними засобами механізмів захисту, досягається певний рівень стійкості кожного з ФПЗ, який гарантується постачальником.

Таблиця 2.1 – Функціональні послуги захисту, які надаються штатним комплексом захисту ЦКС типу EWSD

Специфікації ФПЗ	Найменування ФПЗ
1	2
1. Лавиноподібне зростання кількості телефонних викликів	
Ф01/РДО/Д'Н/АЛ\ПС	Використання змішаної стратегії управління доступом, що застосовується з боку телефонних комутаторів і прикінцевих абонентських пристроїв до сервісних функцій і послуг ЦКС
Ф01/РДО/Д'Н/МО\ПЦ\СК	Використання змішаної стратегії управління доступом, що застосовується з боку моніторів обслуговування до програм, даних, процесів та пристроїв підсистеми управління ЦКС
Ф01/МРК\Д'Н\РР\І	Маркування інформаційних ресурсів ЦКС у разі використання змішаних правил
Ф01/АУД\СК	Аудит (контроль дій суб'єктів) у підсистемі управління ЦКС
2. Несанкціоноване адміністрацією власника ЦКС користування з боку "тіньових" абонентів послугами, що надаються ЦКС EWSD	
Ф01/АНЛ/ПР\АЛ	Аналіз протоколів ідентифікації й автентифікації абонентів ЦКС
Ф01/АУД\АЛ	Аудит (контроль дій абонентів) у підсистемі комутації абонентських каналів зв'язку ЦКС
Ф01/РДО/Д'Н/АЛ\ПС	Використання змішаної стратегії управління доступом, що застосовується з боку телефонних комутаторів і прикінцевих абонентських пристроїв до сервісних функцій і послуг ЦКС
Ф01/АНЛ/ПР\СК	Аналіз лістингів протоколів ідентифікації й автентифікації (перевірки істинності) користувачів підсистеми управління ЦКС
Ф01/АУД\СК	Аудит (контроль дій суб'єктів) у підсистемі управління ЦКС
Ф01/ВЯВ/ТЛ\НК	Виявлення, сигналізація і реєстрація спроб НСД (на термінал адміністратора і порушника)
Ф02/ВЯВ/О\НК\АЛ\А	Застосування індивідуальних засобів виявлення несанкціонованого користування аналоговою абонентською лінією ЦКС
Ф02/ВЯВ/О\НК\АЛ\Ц\Ш	Застосування індивідуальних засобів виявлення несанкціонованого користування цифровою абонентською лінією ЦКС за допомогою штатного цифрового абонентського прикінцевого пристрою
3. Несанкціоноване користування іншими операторами зв'язку послугами, що надаються ЦКС EWSD, за рахунок порушення цими операторами угод щодо порядку оплати для транзитних ЦКС міжстанційного трафіка	
Ф01/БЛК\ОД	Блокування об'єктів доступу при спробі НСД
Ф01/РДО\ОД\СД	Розподіл об'єктів доступу між суб'єктами ЦКС

Специфікації ФПЗ	Найменування ФПЗ
1	2
4. Несанкціонований доступ (НСД): 4.1. НСД до операційної системи (ОС) ЦКС EWSD; 4.2. НСД до програмного забезпечення користувача ЦКС EWSD; 4.3. НСД до програмного забезпечення технічної експлуатації ЦКС EWSD; 4.4. НСД до спеціалізованих програм управління з'єднанням ЦКС EWSD	
Ф01/ВИК\ЗР'ЗМ\ПЗ\Ш	Виключення з операційного середовища ЦКС засобів розробки та налагодження програм, а також засобів спостереження та модифікації об'єктного коду програм
Ф01/ТСТ/Т\ЦЛ\ЗЗ	Періодичні перевірки цілісності засобів бази захисту ЦКС, включаючи контроль цілісності системи розмежування доступу
Ф01/ТСТ/Т\ЦЛ\КФ\ПЗ'ТЗ	Періодичні перевірки цілісності конфігурації програмно-технічних засобів ЦКС
Ф01/ВЯВ/ТЛ\НК	Виявлення, сигналізація і реєстрація спроб НСД (на термінал адміністратора і порушника)
Ф05/МОН\ПЗ'ТЗ\ЗВ\ПЦ	Наявність засобів моніторингу програмно-технічних засобів ЦКС на предмет виявлення позаштатних впливів на програми, дані і процеси на ЦКС
Ф10/ПТД\ПЗ\Щ	Реалізація захисту від можливості завантаження позаштатного програмного забезпечення
3. НСД до технологічних баз даних, що розміщені на комутаційних модулях ЦКС EWSD	
Ф01/РДО/Д'Н/МО\ПЦ\СК	Використання змішаної стратегії управління доступом, що застосовується з боку моніторів обслуговування до програм, даних, процесів та пристроїв підсистеми управління ЦКС
Ф01/ІЗЛ\СЗ	Ізоляція системних засобів ЦКС
Ф01/ІЗЛ\РР\Г	Ізоляція базових засобів ЦКС, тобто станційних ресурсів спільного користування
Ф01/РДО\ОД\СД	Розподіл об'єктів доступу між суб'єктами ЦКС
Ф01/ВЯВ/ТЛ\НК	Виявлення, сигналізація і реєстрація спроб НСД (на термінал адміністратора і порушника)
6. НСД до системного терміналу або АРМу, який приєднано або може бути приєднано до підсистеми управління ЦКС	
Ф01/ІЗЛ\СЗ	Ізоляція системних засобів ЦКС
Ф01/ІЗЛ\РР\Г	Ізоляція базових засобів ЦКС, тобто станційних ресурсів спільного користування
Ф01/РДО\ОД\СД	Розподіл об'єктів доступу між суб'єктами ЦКС
Ф01/АНЛ/ПР\СК	Аналіз лістингів протоколів ідентифікації й автентифікації (перевірки істинності) користувачів підсистеми управління ЦКС
Ф01/АУД\СК	Аудит (контроль дій суб'єктів) у підсистемі управління ЦКС
Ф01/ВЯВ/ТЛ\НК	Виявлення, сигналізація і реєстрація спроб НСД (на термінал адміністратора і порушника)
Ф03/ПВІ/ЗЗ\НМ\ЕУ	Захист ліній зв'язку шляхом застосування захисних пристроїв у критичних елементах устаткування
7. НСД до модемної лінії доступу до модуля технічної експлуатації ЦКС EWSD	
Ф01/РДО/Д'Н/МО\ПЦ\СК	Використання змішаної стратегії управління доступом, що застосовується з боку моніторів обслуговування до програм, даних, процесів та пристроїв підсистеми управління ЦКС
Ф01/АНЛ/ПР\АЛ	Аналіз протоколів ідентифікації й автентифікації абонентів ЦКС
Ф01/АУД\АЛ	Аудит (контроль дій абонентів) у підсистемі комутації

Специфікації ФПЗ	Найменування ФПЗ
1	2
	абонентських каналів зв’язку ЦКС
Ф02/МОН\ЗВ\ПЗ’ТЗ\Ш	Підтримка засобів моніторингу програмно-технічних засобів ЦКС на предмет виявлення позаштатних впливів через штатні засоби
Ф03/ПВІ/ЗЗ\НМ\ЕУ	Захист ліній зв’язку шляхом застосування захисних пристроїв у критичних елементах устаткування
8. НСД до фізичних носіїв інформації із програмним забезпеченням ЦКС	
Ф11/КТР\ЦЛ\ЗЗ	Наявність засобів перевірки автентичності (цілісності) еталонних копій об’єктних модулів бази захисту ЦКС
Ф11/КТР\ЦЛ\ПЗ	Наявність засобів перевірки автентичності (цілісності) еталонних копій об’єктних модулів програмного забезпечення ЦКС
Ф11/РДО\ФН	Розмежування правил доступу до інформації, збереженої на фізичних носіях
Ф11/КТР\ФН	Контроль інформації, збереженої на фізичних носіях
9. НСД до станційного кросу ЦКС EWSD	
Ф03/ПВІ/ЗЗ\НМ\ЕУ	Захист ліній зв’язку шляхом застосування захисних пристроїв у критичних елементах устаткування
Ф04/МОН\ПЗ’ТЗ\ЗВ\ЕУ	Наявність засобів моніторингу програмно-технічних засобів ЦКС на предмет виявлення впливів позаштатними засобами на елементи устаткування ЦКС
Ф10/ВЯВ\НК\ЕУ	Виявлення і реєстрація спроб несанкціонованого доступу до елементів устаткування
Ф10/ПТД\М/РЕ\ЕУ	Наявність механічних засобів, що обмежують фізичний доступ до елементів устаткування ЦКС (нерозбірні зовні шафи, замкові пристрої і т. ін.)
10. Активізація пристроїв: 10.1. Активізація закладних пристроїв і (або) програмних закладок, що встановлені на (у) елементах підсистеми управління на передексплуатаційних стадіях життєвого циклу ЦКС EWSD; 10.2. Активізація нештатних додаткових видів обслуговування (ДВО)	
Ф06/КТР\ЦЛ\ЗЗ\ЗК/ПЗ’ТЗ	Контроль цілісності засобів захисту від програмних і (або) технічних закладних пристроїв
Ф06/МОН\ПЗ’ТЗ\ЗК/ІС	Наявність засобів моніторингу програмно-технічних засобів ЦКС на предмет виявлення закладних пристроїв, а також сигналів, що ініціюють їхню активізацію
Ф10/ПТД\ТЗ\ЗК	Наявність конструкції, що утруднює можливість установлення закладних пристроїв (мінімальний вільний простір, компаунди, запаяні кожухи і т. ін.)
Ф10/ВКР/ПЗ/М	Використання модульності програмного забезпечення
Ф03/ПТР\ТР	Підтримка оптимальної температури навколишнього середовища ЦКС
Ф03/НТР\ЕП	Виявлення і реєстрація відхилень параметрів енергопостачання ЦКС

Рівень стійкості механізму захисту, який реалізують ФПЗ стосовно спроб його безпосереднього злому, позначається однією цифрою від 1 до 3. При цьому:

1 – позначає мінімальний (базовий) рівень стійкості механізмів захисту;

2 – позначає середній рівень стійкості механізмів захисту;

3 – позначає високий рівень стійкості механізмів захисту.

Специфікація ФПЗ (рівня стійкості механізму захисту) на АТС – це опис технічних вимог, показників функціонування, нормуючих та обмежуючих умов, яких слід дотримуватися в процесі реалізації цієї ФПЗ (цього механізму захисту), якщо оцінка рівня захищеності інформаційних ресурсів АТС виконується або буде виконуватися відповідно до вимог.

2.6.5 "Слабкі місця" системи технічного захисту інформаційних ресурсів у ЦКС типу *EWSD*

Знайдені під час проектування КСЗІ «слабкі місця» системи технічного захисту інформаційних ресурсів у цифровій комутаційній системі типу *EWSD* та засоби нейтралізації «слабких місць» наведені у табл. 2.2.

Слабке місце у захисті – сертифікований канал можливої реалізації загроз для інформаційних ресурсів, механізми захисту для протидії котрим у системі ТЗІ відсутні.

Таблиця 2.2 – «Слабкі місця» системи технічного захисту інформаційних ресурсів у ЦКС типу *EWSD*

Характеристики слабкого місця	Заходи для нейтралізації "слабкого місця"
1. Термінал технічного обслуговування та експлуатації ЦКС являє собою персональний комп'ютер, який може бути укомплектовано пристроєм для читання інформації з зовнішніх носіїв. Наявність цього пристрою надає змогу завантаження у систему позаштатного програмного забезпечення , яке може бути використане порушником з метою створення загроз інформаційним ресурсам	Виключати з конфігурації термінала технічного обслуговування та експлуатації або захищати від можливого використання пристрої для читання позаштатного програмного забезпечення
2. Термінали технічного обслуговування та експлуатації можуть бути підключені за допомогою модемів через загальну телефонну мережу, що надає змогу дистанційного обслуговування ЦКС. Така можливість може бути використана порушником з метою створення загроз інформаційним ресурсам	Не залишати без необхідності підключені до терміналів модеми та слідкувати під час сеансів дистанційного обслуговування ЦКС за наявністю повноважень користувачів

Вилом у захисті – сертифікований канал можливої реалізації загроз для інформаційних ресурсів, механізми захисту для протидії котрим у системі ТЗІ присутні, але перебувають у непрацюючому стані.

Прикладом «слабкого місця» в захисті може бути модифікація з боку підсистеми управління порядку (або умов) роботи інформаційно-вразливих режимів, функцій і послуг, що надаються АТС, з метою реалізації загроз на підсистемі КАЗЛ станції.

Для забезпечення коректності (тобто, слушності) реалізації створеного на АТС комплексу засобів і механізмів захисту, всі виявлені «слабкі місця» та

виломи у захисті повинні бути нейтралізовані. В процесі атестації системи ТЗІ на АТС проводяться роботи з аналізу на відсутність «слабких місць» у захисті.

Заходи для нейтралізації «слабких місць», у даному випадку мають бути реалізованими позасистемним методом.

2.6.6. Загальні заходи захисту в комплексній системі захисту інформації в ЦКС типу *EWSD*

Комплексна система захисту інформації (КСЗІ) складається із штатних (спеціальних) заходів та механізмів захисту (КЗМЗ) та загальних засобів захисту, які реалізуються у будь-якій системі захисту і доповнюють КЗМЗ до функціонально повної КСЗІ.

Вимоги до системи технічного захисту, яка реалізується на ЦАТС, формуються наступним чином. Відповідно до принципу мінімальної достатності (НД ТЗІ 1.1-001) система захисту повинна бути спроектована так, щоб здійснювалася протидія тільки тим загрозам, що мають суттєве значення для держави, операторів електрозв'язку та абонентів, і тільки в тій мірі, у котрій необхідно нейтралізувати (послабити, зменшити) наслідки прояву таких суттєвих загроз для того, щоб втрати від їхніх можливих реалізацій не перевищили гранично допустимих рівнів.

ЦАТС, як правило, оснащується штатними і, при необхідності, додатковими (позаштатними) засобами ТЗІ, які при їхньому спільному використанні утворюють комплекс засобів і механізмів захисту (КЗМЗ), що забезпечує потрібний рівень захищеності її інформаційних ресурсів.

Модель захисту є функціонально повною, тобто у моделі захисту відсутня хоча б одна суттєва загроза, для якої не була б організована протидія за допомогою хоча б однієї ФПЗ чи загального механізму захисту.

Запитання для самоконтролю

1. На що спрямовано технічний захист інформації?
2. Поясніть узагальнену модель інфраструктури цифрового вузла комутації з позицій технічного захисту інформації.
3. Поясніть структурну схему станційної частини програмно-керованої АТС з позицій ТЗІ.
4. Прокоментуйте основні загрози інформаційним ресурсам вузла комутації.
3. Опишіть типову модель порушника.
6. Які можливі загрози інформаційним ресурсам ЦАТС від приєднаних технологічних загроз?
7. Які можливі варіанти нападу на мережі зв'язку?
8. Опишіть загрози, які реалізуються через систему сигналізації.
9. Опишіть загрози, що реалізуються за допомогою системи централізованого управління.
10. Опишіть загрози на абонентських та з'єднувальних лініях.
11. Сформулюйте вимоги до забезпечення інформаційної безпеки програмно-керованої АТС.
12. Яка мета діяльності щодо забезпечення інформаційної безпеки ЦАТС?

13. Поясніть принципи діяльності щодо забезпечення інформаційної безпеки ЦАТС.

14. Які є пріоритети забезпечення інформаційної безпеки ЦАТС?

13. Які є головні завдання діяльності в сфері ТЗІ?

16. Поясніть головні напрямки діяльності із забезпечення інформаційної безпеки ЦАТС.

4. Для чого і як проводиться атестація системи захисту інформації в ЦАТС?

18. Як виконується управління системою інформаційної безпеки?

19. Які засоби впровадження комплексу засобів захисту є первинними та основними?

20. Яка послідовність робіт із впровадження комплексу заходів й засобів захисту?

21. Поясніть організацію технічного захисту інформації на стадії побудови ЦАТС.

22. Поясніть організацію технічного захисту інформації на стадії вводу в експлуатацію ЦАТС.

23. Поясніть організацію технічного захисту інформації на стадії технічної експлуатації ЦАТС.

24. Наведіть схему організації та забезпечення ТЗІ ЦАТС та телекомунікаційних мереж.

3 РЕАЛІЗАЦІЯ МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЇ В ПРОГРАМНО-КЕРОВАНИХ АТС

Далі у цьому розділі розглядається конкретний приклад реалізації механізмів технічного захисту інформації в ЦАТС типу *EWSD*.

3.1 Розподіл задач, функцій та механізмів захисту інформації ЦАТС типу *EWSD*

З точки зору інформаційної безпеки цифрові АТС розглядаються комплексно разом із системою її управління та її зв'язками з мережею та навколишнім середовищем. Система управління станції *EWSD* станції є складною системою, її спрощена схема показана на рис. 3.1. Управління станцією може здійснюватись безпосередньо з її території і віддалено з центра управління мережею. У обох випадках управління здійснюється через телекомунікаційні інтерфейси. Система управління включає в себе мережу передачі даних (у межах станції та/або у межах місцевої телекомунікаційної мережі), ЛОМ центра управління мережею та ЛОМ віддаленого управління мережею.

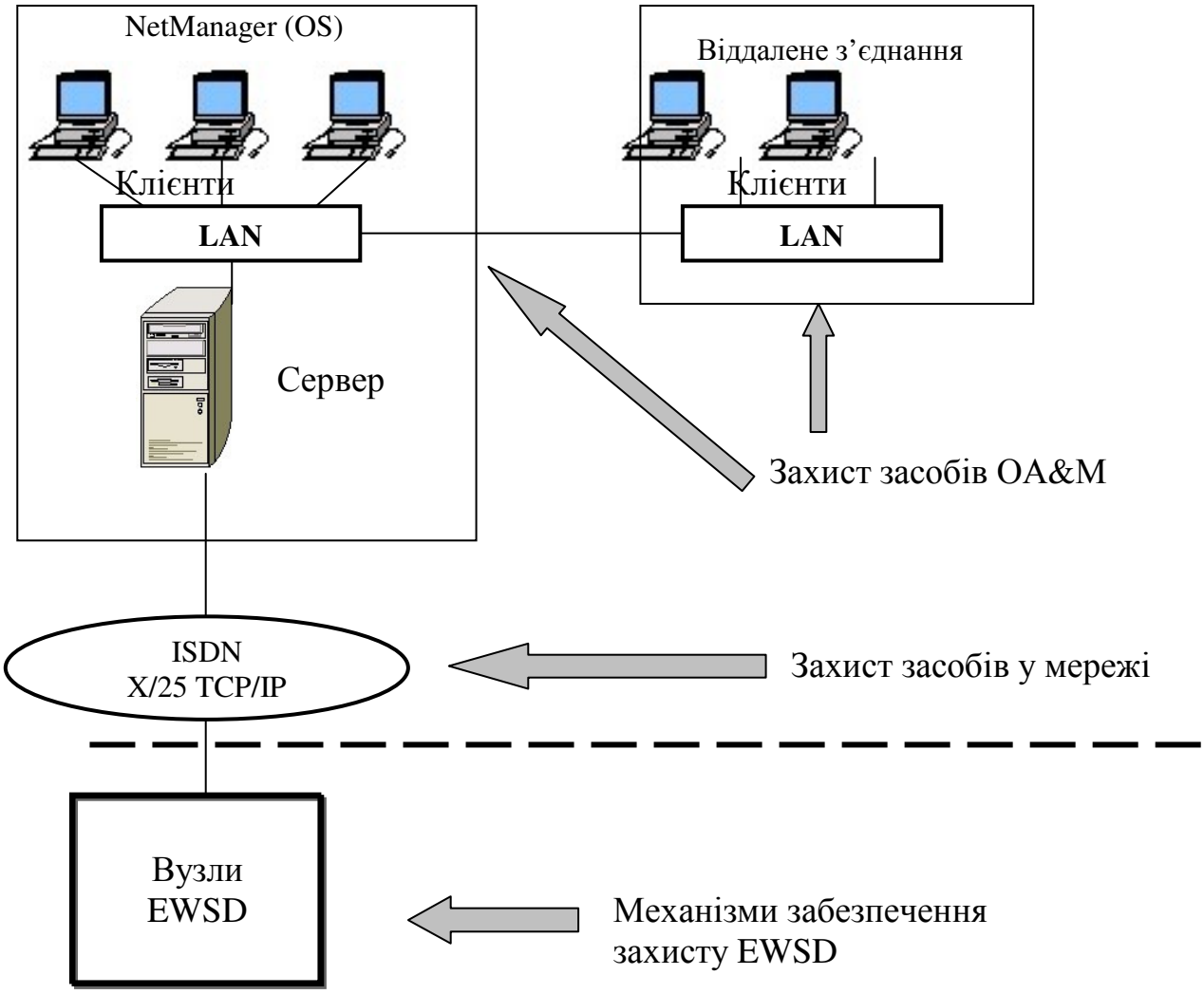

Рисунок 3.1 – Розподіл функцій захисту між вузлом *EWSD* і системою управління

Для управління станції *EWSD* через мережу передачі даних загального користування використовуються мережні протоколи X.25 (за необхідністю реалізуються через *ISDN*) та/або *TCP/IP*. Протокол *TCP/IP* використовується в конфігурації *EWSD PowerNode* або *Standalone STP* (автономний *STP*). У цьому випадку використовується інтерфейс *TCP/IP* процесора *MP*.

OA&M (*Operations, Administration, and Management* (*or sometimes Maintenance*) – експлуатація, адміністрування, менеджмент або підтримка) – це загальний термін, що описує процеси, дії, інструменти, стандарти тощо, залучені до експлуатації, адміністрування та менеджменту чи підтримки якої-небудь системи. Як правило, вона використовується з комп'ютерними мережами та комп'ютерним апаратним забезпеченням.

NetManager – включає в себе адміністрування бази даних маршрутизації мережевих елементів *EWSD* (створення "маршруту" для проходження трафіку від відправника до одержувача), адміністрування бази даних ОКС 7 мережних елементів, конфігурування елементів вузла комутації та периферійних пристроїв; адміністрування аналогових, *ISDN*, *H*323, *VoDSL* абонентів, таксофонів, УАТС, мереж доступу, абонентських сервісів та обладнання,

управління аварійними ситуаціями. Програма виконує моніторинг стану всіх елементів EWSD, виводячи на монітор аварії з класифікацією за ступенем критичності (warning, major, critical), при цьому супроводжуючи звуковим сигналом непідтверджені аварії. Також дозволяє в режимі реального часу реагувати на аварійні ситуації, тим самим мінімізуючи час недоступності сервісу, керування користувачами та збір статистики.

Інші скорочення та умовні позначення подані у розд. «Умовні позначення та скорочення» в кінці навчального посібника.

Задачі забезпечення захисту реалізуються за допомогою функцій захисту. Функції захисту реалізуються механізмами захисту, а механізми захисту реалізуються прикладними програмами і/або апаратними (технічними) засобами.

Функції забезпечення захисту, що використовуються під час експлуатації вузлів *EWSD* у відкритих комп'ютерних мережах, поділяються на такі категорії:

- механізми забезпечення захисту в *EWSD*;
- захист даних у мережі (*IP*-захист в мережах *TCP*/*IP*);
- захист засобів *OA&M*, що розглядається в іншому навчальному посібнику.

Розглянемо докладніше специфікації функцій кожної з категорій та механізмів захисту за умови використання в системі управління станцією операційної системи *Windows NT*.

3.2 Функції та механізми забезпечення захисту в *EWSD*

Для вирішення комплексу задач захисту в *EWSD* реалізують наступні функції захисту:

- захист функціонування вузла *EWSD*;
- захист функціонування з використанням *MML*;
- захист функціонування з використанням *Q*3;
- адміністративна програма для *MML*-команд;
- захист спеціальних програм;
- захист файлів;
- захист під час передачі файлів.

3.2.1 Захист функціонування вузла *EWSD*

Кожна з функцій захисту вузла реалізується за допомогою механізмів забезпечення захисту *EWSD*, що складаються з таких компонентів:

- захист доступу до системи в *NetManager*;
- захист доступу до системи в мережному вузлі *EWSD*;
- захист доступу до даних;
- перевірка спостережності;
- виведення аварійних звітів.

Захист доступу до системи в NetManager. Захист доступу дозволяє запобігти несанкціонованому відкриттю сеансів у *NetManager*. В основу реалізації захисту доступу покладені механізми забезпечення захисту, визначені в операційній системі *Windows NT*.

Нижче наведені основні специфікації механізмів забезпечення захисту в *NetManager*:

- Повноваження адміністратора в операційній системі *Windows NT* встановлюються під час інсталяції *NetManager* за допомогою автоматичного призначення імен групам користувачів *Windows NT*. Користувачі, які відносяться до групи "Адміністратори *ENM*" ("*ENM Administrators*") системи *NetManager*, мають повноваження адміністраторів кожного комп'ютера в операційній системі *NetManager*. Група користувачів "Адміністратори *ENM*" домену *NT* є частиною локальної групи адміністраторів на всіх комп'ютерах *NetManager*. Усі користувачі *NetManager* призначаються групі "Користувачі *ENM*" ("*ENM Users*") домену *Windows NT*.

- Первісне призначення повноважень адміністратора в операційній системі *NetManager* виконується під час інсталяції *NetManager* за допомогою спеціальних груп користувачів *NetManager* (на відміну від групи користувачів *Windows NT*).

- Ім'я користувача, під яким виконується інсталяція і ім'я користувача, визначене як "Адміністратор *ENM*" в процесі інсталяції, автоматично додаються до групи користувачів "Адміністратори *ENM*" *NetManager*.

- Адміністратор призначає всі інші повноваження шляхом адміністрування груп користувачів *NetManager*.

На специфічній для користувача основі призначаються тільки програмні *NetManager*:

- користувачі реєструються в операційній системі під час їх реєстрації у *Windows NT*. Користувачі можуть звертатися до всіх програм і мережним вузлам *EWSD*, які їм були призначені адміністратором.

- механізми забезпечення захисту доступу для мережних вузлів *EWSD* відповідають аналогічним механізмам відповідної версії *EWSD*. Адміністратор призначає права користувача мережного вузла групі користувачів *NetManager*. При призначенні прав користувача мережного вузла за основу беруться параметри, встановлені в базі даного вузла.

- інформація, пов'язана з доступом до мережних вузлів *EWSD*, зберігається в закодованій формі в центральній базі даних системи захисту в операційній системі. Ця інформація автоматично використовується для надання доступу до мережних вузлів *EWSD*. Під час надходження з мережного вузла *EWSD* запиту на цю інформацію процес конфігурування *NetManager* автоматично змінює паролі на довільній основі. Це дозволяє уникнути закінчення терміну дії паролів і запобігає повторне використання паролів, придбаних "незаконним шляхом", для несанкціонованого доступу до системи.

Захист доступу до системи в мережному вузлі EWSD. Захист доступу до системи запобігає несанкціоноване відкриття сеансів в мережних вузлах *EWSD*. Для реалізації захисту доступу до системи використовуються наступні засоби:

- ідентифікація ініціаторів. *EWSD* класифікує віддалених операторів, пристрої/процесори або застосування як ініціаторів. Кожному ініціатору присвоюється індивідуальний ідентифікаційний код. Цей код повинен бути введений для ідентифікації ініціатора під час відкриття сеансу;

- аутентифікація за допомогою паролю. Кожен ініціатор проходить аутентифікацію за допомогою персонального пароля. Для кожного ідентифікатора ініціатора може бути вибраний і призначений будь-який пароль. Для запобігання "викрадення" паролів і їх несанкціонованого повторного використання можлива їх передача з

використанням процедур динамічного шифрування (зашифрований пароль), за допомогою яких пароль шифрується разом з поточним часом доби і деяким випадковим числом. У випадку "викрадення" пароля він не може бути використаний повторно для отримання (несанкціонованого) доступу до системи.

Процедури ідентифікації та аутентифікації показані на рис. 3.2.

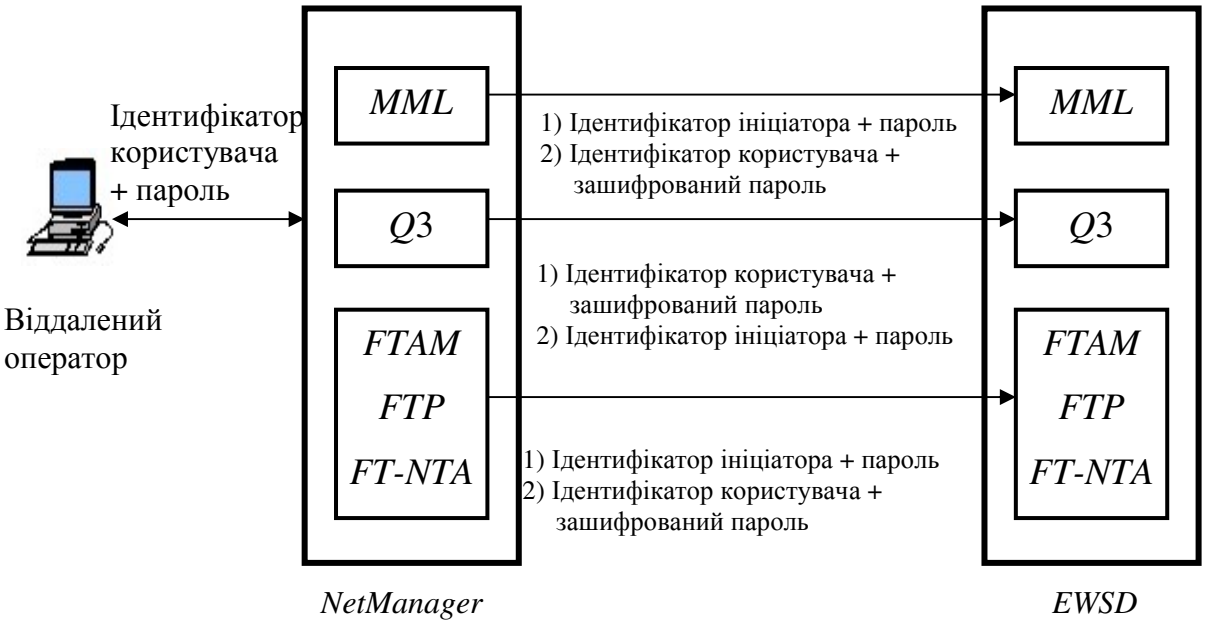

Рисунок 3.2 – Процедури аутентифікації

Захист доступу до даних. Захист доступу до даних запобігає несанкціоноване виконання команд і несанкціонований доступ до системних ресурсів, наприклад до файлів. Захист доступу до даних реалізується наступними засобами:

- призначення дозволів на MML команди для ідентифікаторів користувачів, програм та пристроїв;
- призначення дозволу на доступ для виконання Q3-операцій;
- захист файлів при отриманні доступу до них.

Перевірка спостережності. Для забезпечення перевірки спостережності можлива автоматична реєстрація наступних дій:

- відкриття сеансу;
- введення критичних операцій;
- доступ до файлів.

Перевірка очевидності дозволяє приймати рішення і робити висновки з приводу виконаних або зроблених спроб неправильного використання повноважень після настання події, що дозволяє вжити відповідних заходів з відновлення захисту.

Виведення аварійних звітів.

Про факти потенційного порушення захисту, наприклад, спроба відкриття сеансу з використанням недійсного пароля або операції, відхилені внаслідок недостатності прав доступу, передаються повідомлення у вигляді аварійних сигналів, а також здійснюється запис відповідної інформації у файл реєстрації.

Залежно від типу порушення прав доступу до системи або порушення доступу до даних можуть робитися наступні дії з відновлення системи захисту:

- передача аварійних сигналів оператору системи;
- блокування пристроїв / процесорів;
- блокування ідентифікаторів користувачів;
- завершення сеансу.

3.2.2 Захист функціонування з використанням *MML*

Засоби захисту функціонування з використанням *MML* складаються з наступних компонентів:

- захист доступу до системи;
- захист доступу до даних;
- перевірка спостережності;
- виведення аварійних звітів.

Захист доступу до системи. Захист доступу до системи запобігає встановлення локальними клієнтами *NetManager*, підключеними до координаційного процесору *EWSD*, несанкціонованих діалогових сеансів при використанні *MML.* Ця функція реалізується за допомогою таких засобів:

- ідентифікація користувачів. Ідентифікатор користувача містить від 4 до 8 символів. Всі ідентифікатори користувачів, які використовуються в одному вузлі, повинні мати однаковий розмір, значення якого визначається при створенні першого *ID*. Може бути створено до 400 ідентифікаторів користувачів;
- аутентифікація за допомогою паролю. Пароль - це символьний рядок, що складається з 4 - 24 символів, що привласнюється виключно одному користувачеві і відомий тільки йому. Паролі повинні складатися принаймні з 4 символів та містити принаймні один цифровий символ, один спеціальний символ і одну букву.

Резервна копія всіх ідентифікаційних і аутентифікаційних даних зберігається у файлі, що не є специфічним для конкретної генерації. Це забезпечує постійне підтримання актуальності цих даних незалежно від генерації навіть після аварійного повернення до попередньої генерації в режимі *on-line*.

Захист доступу до даних. Захист доступу до даних запобігає несанкціоноване виконання *MML* команд. Для реалізації цієї функції використовуються наступні засоби:

- класи повноважень для *MML* команд. *MML* команди згруповані в класи повноважень відповідно до реалізованих ними функціями. Існує 50 класів повноважень. Адміністрування класів 2 - 49 може виконуватися відповідно до конкретних вимог користувача. Клас повноважень 1 є класом за замовчуванням і містить всі *MML* команди. У класі повноважень 50 містяться ті команди, які необхідні для підтримки постійної роботи системи. Ці класи повноважень не можуть бути змінені оператором.;
- повноваження. Повноваження - це група, що складається з декількох класів повноважень. Саме ці повноваження призначаються пристроям або ідентифікаторам користувачів. Існує 51 повноваження. Для запобігання виведення системи з ладу в результаті введення команд оператором передбачено три фіксовані повноваження. Повноваження "0" не містить будь-яких класів повноважень, повноваження "1"

містить клас повноважень 1 для всіх команд. Повноваження "SYSOUT" містить клас повноважень 50. Решта 48 повноважень можуть бути визначені довільно шляхом призначення класів повноважень. Принципи призначення повноважень ілюстровані рис. 3.3:

- адміністрування прав доступу Адміністрування *MML* прав дозволяє призначати повноваження користувача та повноваження пристроїв та повноваження програм. Повноваження користувача визначає команди і програми, які дозволено виконувати даному конкретному користувачу. Повноваження пристроїв та програм визначають команди, які дозволено виконувати системі *NetManager* або застосуванням віддаленого процесора;

- верифікація прав для *MML* команд Для всіх команд виконується верифікація прав. Перш ніж обробляти команду, система перевіряє, чи дозволено її виконання для даного конкретного користувача й пристрою. Набір дозволених команд визначається на підставі повноважень користувачів та пристрою під час відкриття сеансу ;

- верифікація прав для *COFIP*-завдань. *COFIP*-завдання можуть бути створені тільки в діалоговому сеансі. Для команди, яка використовується при створенні цих завдань, також виконується верифікація прав, і ця команда може бути виконана тільки в тому випадку, якщо вона включена в повноваження сеансу. Це ж правило відноситься і до тих команд, які виконуються за допомогою процесора командних файлів (*COFIP*).

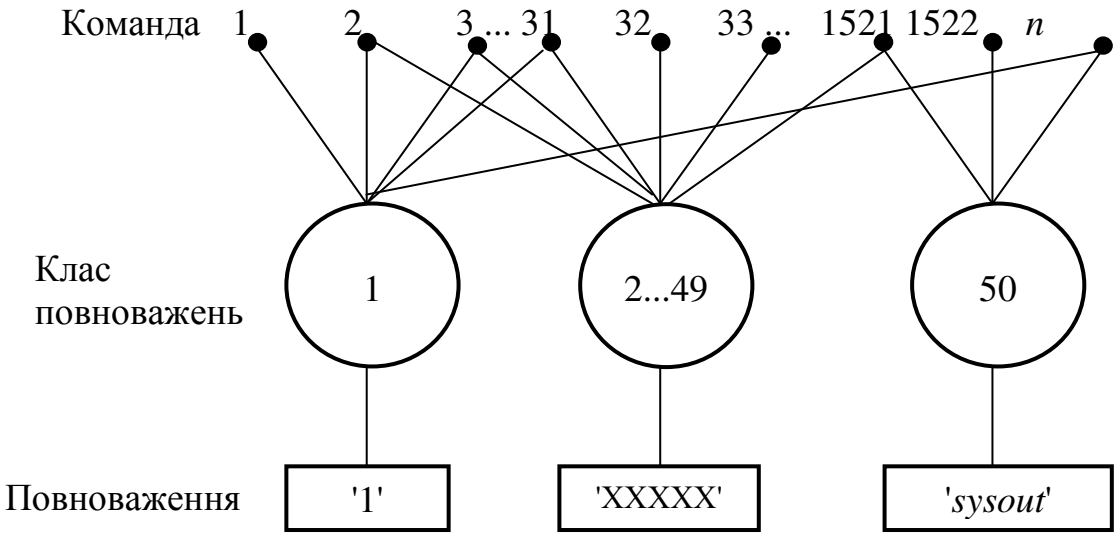

Рисунок 3.3 – Призначення команд повноважень

Структура повноважень сеансу показана на рис. 3.4.

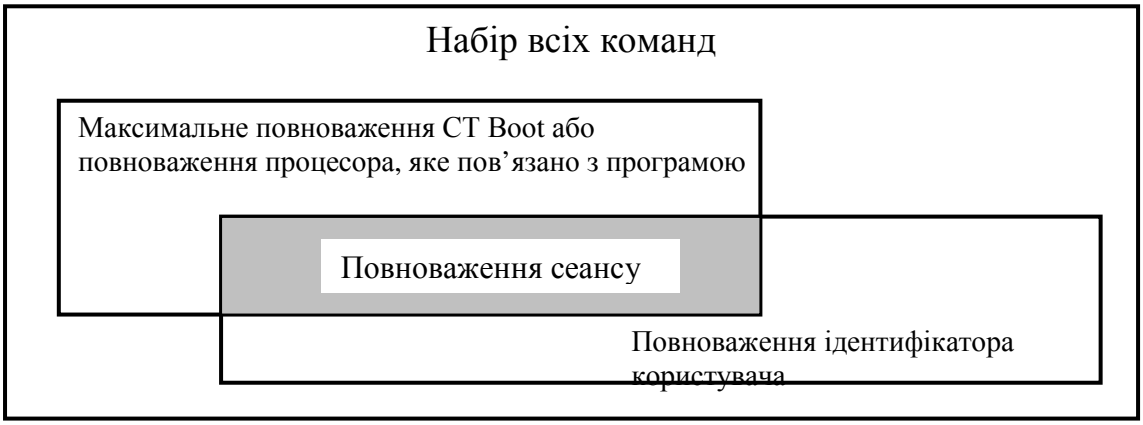

Рисунок 3.4 – Структура повноваження сеансу

Сеанс для запланованих *COFIP*-завдань не відкривається до тих пір, поки не буде розпочато виконання завдання. Повноваження сеансу надсилається з того діалогового сеансу, в якому було створено завдання. Щоб уникнути подальших змін або маніпуляцій процесор командних файлів забезпечує захист командного файлу від перезапису чи видалення під час створення запланованого *COFIP*-завдання.

Якщо користувач був блокований в період часу між створенням COFIP-завдання і моментом його запланованого виконання, то встановлюється відмінність між ідентифікаторами користувачів, блокованими по команді, введеної оператором, і ідентифікатори користувачів, блокованими автоматично внаслідок введення невірного пароля або введення несанкціонованої команди. При цьому запити *COFIP* не обробляються внаслідок блокованого ідентифікатора користувача тільки в тому випадку, якщо цей *ID* був блокований через введення санкціонованої команди.

Цей спосіб дозволяє забезпечити не тільки неможливість зупинки обробки запланованих COFIP-завдань в результаті "дій з боку несанкціонованих користувачів" (введення невірного пароля), але він дозволяє також розпізнавати і не допускати спроб порушення правил доступу "санкціонованими" користувачами (введення несанкціонованої команди).

Перевірка спостережності. Для перевірки "спостережності" використовуються два циклічних файла. Один файл призначений для реєстрації введених недійсних паролів, а другий для реєстрації подій відкриття сеансу і спроб введення несанкціонованих команд. При цьому реєструються наступні дані: позначення вузла *EWSD*; подія; дата; час; ідентифікатор користувача; ідентифікатор пристрою; повтор введеної команди.

Ініціатор дії може бути ідентифікований за допомогою параметра *'user ID*' ('ідентифікатор користувача') і *'device ID'* ('ідентифікатор пристрою').

Реєстрація введення невірного пароля не може бути деактивована і не може бути обмежена тільки будь-якими специфічними користувачами.

Реєстрація подій відкриття сеансу і спроб введення несанкціонованих команд може бути обмежена довільно вибраними користувачами та / або віддаленими процесорами / пристроями.

Виведення аварійних звітів. Для наступних порушень правил доступу здійснюється поточний контроль за граничним значенням:

- введення невідомих ідентифікаторів користувачів. Якщо на одному і тому ж робочому пристрої послідовно вводиться кілька невизначених ідентифікаторів користувачів та загальне число неправильно введених значень досягає граничного значення, то термінал автоматично блокується на дві хвилини. Блокування не відображається у вигляді аварійного сигналу на дисплеї стану системи. Блокування не може бути скинуте. Запити на проведення сеансу, дані під час блокування пристрою, відхиляються;

- введення невірних паролів користувача. Для контролю функціонування координаційного процесора в *EWSD* можна встановити (у "шаховому" порядку) тривалість блокування з часовими межами. Може бути встановлено п’ять рівнів. Рівень 5 завжди означає блокування без обмежень. Санкціонований користувач (системний адміністратор) може встановлювати порогове значення для першого рівня блокування і скидати блокування. Загальна тривалість блокування для ідентифікаторів системних адміністраторів обмежена максимум 2 хвилинами. Блокування цього *ID* завжди відображається на дисплеї стану системи у вигляді аварійного сигналу. Аварійний сигнал реєструється також у файлі хронологією;

- введення несанкціонованих команд. Якщо кількість повторних введень несанкціонованих команд перевищує порогове значення, то це призводить до блокування ідентифікатора і припинення діалогового сеансу. У цьому контексті до несанкціонованих команд відносять ті команди, які мають правильний синтаксис, але не відображені в повноваженні сеансу. У цьому випадку також може бути встановлена тривалість блокування (у шаховому порядку) з часовими межами.

Можливе встановлення порогових значень для порушень правил доступу. Блокування, що ініціюються системою, можуть бути скинуті користувачами з відповідними повноваженнями.

3.2.3 Захист функціонування з використанням *Q*3

Принцип забезпечення захисту в *EWSD* заснований на спільному використанні функцій для користувача системою (*NetManager*) і станцією *EWSD*. Адміністрування профілів повноважень окремих користувачів здійснюється в *NetManager*. Отже, *NetManager* виконує також поточний контроль доступу до застосувань.

EWSD контролює доступ застосувань до об’єктів у базі даних *EWSD*. Програми ідентифікуються за допомогою своєї функції ідентифікації.

Система *NetManager* повинна підтримувати механізм захисту, що реалізується за допомогою зашифрованих паролів, у тому випадку, якщо аутентифікація повинна виконуватися в *Q*3-інтерфейсі користувача під час встановлення асоціації мережевого елемента на платформі *OA&M*. Інші операційні системи повинні забезпечувати підтримку механізму захисту, що реалізується на основі простих паролів. Функції *Q*3-захисту пояснюються за допомогою рис. 3.5.

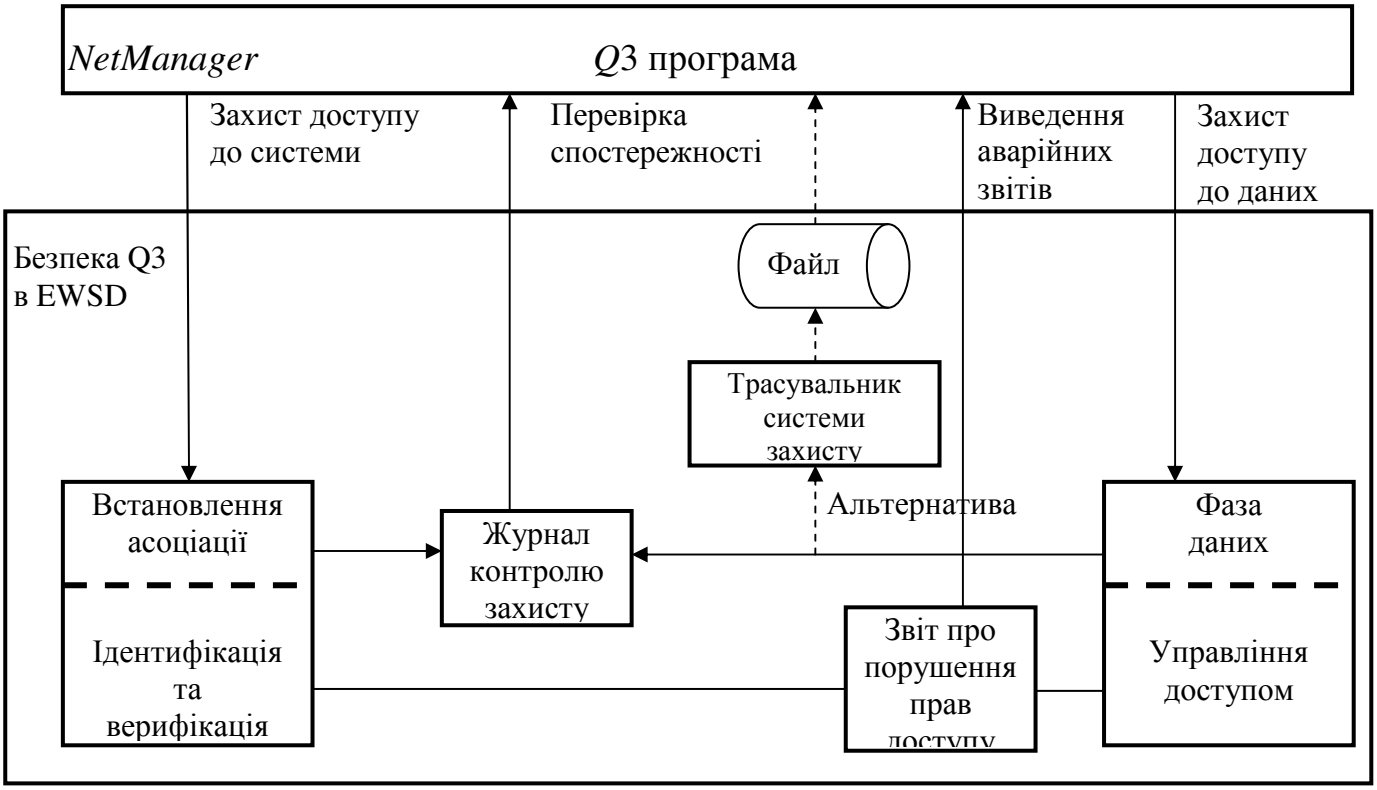

Рисунок 3.5 Функції *Q*3- захисту

Функції Q3-захисту розбиті на чотири області:

- захист доступу до системи для встановлення асоціації (аутентифікація);
- захист доступу до даних, що реалізуються у фазі даних асоціації (управління доступом);
- перевірка спостережності для реєстрації (журнал контролю захисту або трасировщик системи захисту)
- виведення аварійних звітів, це функція захисту виведення аварійних звітів (звіт про порушення прав доступу).

Захист доступу до системи. Ці функції забезпечення захисту ідентифікуються за своїми адресними даними при кожному встановленні асоціації, що виконується віддаленою комп'ютерною системою або *NetManager*. Ідентифікація та аутентифікація виконуються відповідним чином. Існує кілька механізмів перевірки аутентифікації і, таким чином, може бути визначений необхідний для використання механізм у відповідності з кожним окремим ініціатором. Журнал контролю захисту забезпечує реєстрацію навіть тих подій, аспекти захисту яких відноситься до аутентифікації.

Система-партнер ідентифікується і аутентифікується при встановленні вхідної асоціації.

Залежно від використовуваного механізму аутентифікація необхідна для цього: аутентифікаційна інформація передається і порівнюється з еталонними даними, призначеними у вузлі.

Можливо адміністрування наступних механізмів аутентифікації в інтерфейсі користувача *OA & M*:

- Механізм захисту за допомогою зашифрованих паролів ідентифікує систему-партнера з використанням функції ідентифікації та аутентифікує її з використанням

зашифрованого пароля. Для пароля використовується одностороннє шифрування спільно з "*ID*" (наприклад, функція ідентифікації), потім додається тимчасова мітка і деяке випадкове число, після чого знову використовується функція одностороннього шифрування. Включення тимчасової мітки і випадкового числа забезпечує користувачеві неоднакові результати верифікації пароля для кожного сеансу передачі (захист від спроб використання пароля після завершення з'єднання). Тимчасова мітка і випадкове число також повинні передаватися без шифрування для того, щоб на стороні одержувача також можна було вирахувати результуючу комбінацію.

- Механізм захисту за допомогою простих паролів ідентифікує систему-партнера з використанням функції ідентифікації та аутентифікує її з використанням простого пароля. У цьому випадку передається тільки "простий" пароль, представлений у вигляді повного тексту або закодований методом одностороннього шифрування. Такий механізм не забезпечує захист від повторного використання пароля.

Для ініціаторів всіх механізмів аутентифікації доступ може бути наданий у залежності від часу (наприклад, доступ тільки в робочий час, у нічний час, у святкові дні і т.д.).

Залежно від результатів верифікації системі-партнеру надсилаються повідомлення про прийняття або про відхилення з'єднання. Якщо спроба встановлення з'єднання відхиляється через нестачу прав доступу або недійсних аутентифікаційних даних, то виводиться звіт про порушення прав доступу.

Захист доступу до даних. Функція управління доступом до *Q*3 виконує перевірку всіх *Q*3-операцій, що реалізуються після успішної ідентифікації і аутентифікації. Верифікація прав доступу виконується за допомогою алгоритмів доступу, які зберігаються в базі даних системи захисту і використовуються для управління доступом.

Алгоритми доступу пов’язують між собою:

- функції ідентифікації віддаленого NetManager;
- класи об'єктів, до яких здійснюється доступ;
- дозволені й заборонені *Q*3-операції;
- будь-які граничні значення, що обмежують доступ заданим часом дня і / або днями тижня.

Якщо прав доступу не досить, *Q*3-операція відхиляється. У цьому випадку виводиться також аварійний сигнал порушення прав доступу.

Призначення прав доступу до бази даних системи захисту здійснюється адміністратором системи захисту. Управління правами доступу виконується за допомогою *Q*3-операцій. Доступ до самої бази даних системи захисту також "захищений" контролером доступу *Q*3.

Перевірка спостережності. Журнал контролю захисту (в конфігураціях EWSD powernode / standalone STP). Функція контролю захисту генерує повідомлення журналу контролю захисту, які можуть передаватися і зберігатися для реєстрації випадків надання доступу до *Q*3:

- повідомлення журналу контролю генеруються під час фази даних для тих операцій, за допомогою яких модифікується база даних. Ця функція є альтернативним варіантом для трасувальника системи захисту; здійснюється реєстрація тих же самих даних у вигляді службового звіту у файлі реєстрації *Q*3, а не в файлі з результатами

трасування системи захисту.

- можлива реєстрація подій доступу до системи (успішна і безпомилкова аутентифікація) віддалених програм.

Обсяг реєстрованих даних може бути встановлений в залежності від виконуваної фази.

Крім того, для перевірки спостережності використовується *трасувальник системи захисту*. Всі *Q*3-операції, за допомогою яких модифікується база даних, можуть бути зареєстровані за допомогою трасувальника системи захисту. Дані трасування зберігаються в певному файлі файлової системи *EWSD*. При перевищенні порогових значень, визначених для рівня заповнення файлу, генеруються відповідні аварійні сигнали. Для аналізу файлу з результатами трасування системи захисту потрібна програма пост-обробки, яка виконується на зовнішньому комп'ютері. Можливе транспортування цього файлу з використанням протоколу передачі файлів.

Виведення аварійних звітів. Зокрема, виводиться звіт про порушення прав доступу. Інформація про всі порушення захисту, виявлених за допомогою аутентифікації і функції управління доступом, оформляється у вигляді звітів про порушення прав доступу. Звіти про порушення прав доступу є повідомлення, які можуть бути передані і збережені в пам'яті системи.

3.2.4 Адміністративна програма для *MML* -команд

Обробка інформації, обмін якою здійснюється між *NetManager* та вузлами *EWSD*, виконується з використанням стека *OSI*-протоколів на основі протоколу *CMIP*. Передача *MML* команд виконується тільки за допомогою *CMIP*-протоколу. Отже, механізми забезпечення захисту відповідають компонентам, описаним в розділі 3 "Захист функціонування з використанням *MML*".

3.2.5 Захист спеціальних програм

Для спеціальних застосувань, взаємодіючих з координаційним процесором у вузлі *EWSD* за рамками сеансу (наприклад, застосування *TMM*, відмінні від програм управління командами), також вимагається дотримання певних заходів захисту. Адміністрування, що використовуються в програмах ідентифікаторів користувачів і паролів виконується точно так само, як для *MML*. Засоби захисту спеціальних застосувань складаються з наступних компонентів:

- захист доступу до системи. Якщо з'єднання встановлюється віддаленою процесорною системою або системою *NetManager*, воно ідентифікується з мережевою адресою. Якщо процесор-партнер відомий системі *EWSD*, то ідентифікація і аутентифікація виконуються з використанням одночасно передаючих ідентифікатора користувача і пароля;

- захист доступу до даних. Відповідна програма віддаленого процесора має адмініструватися у вузлі *EWSD* і забезпечувати можливість відображення на локальний додаток для реалізації доступу з метою пошуку спеціального застосування. В іншому випадку спроба доступу відхиляється ще на етапі встановлення з'єднання. Крім того, ідентифікатор користувача повинен мати повноваження на виконання цього конкретного, спеціального (локального) застосування;

- перевірка спостережності. Ця функція описана в розділі 3.2.2.

- виведення аварійних звітів. Контролюються наступні порушення правил доступу: введення невідомих ідентифікаторів користувачів згідно з описом у розділі 3.2.2; введення невірних паролів користувача у відповідності з описом в розділі 3.2.2; несанкціоновані виклики спеціальної програми. Повторні несанкціоновані спроби виконання програми призводять до блокування ідентифікатора у разі досягнення граничного значення.

3.2.6 Захист файлів

Засоби захисту файлів складаються з таких компонентів:

- захист файлів у файловій системі *CP*;
- захист файлів, пов'язаних з ініціаторами;
- захист файлів, пов'язаних з паролями;
- виведення аварійних звітів.

Захист файлів у файловій системі CP. Забезпечення захисту файлів, що зберігаються на жорсткому диску *EWSD*, реалізується на основі наступної наявної інформації про захист:

1) захист сегментів імен файлів;

2) атрибути захисту файлів;

3) псевдоніми.

Якщо робиться спроба звернення до файлу, то можливість отримання доступу до нього визначається спільно всіма елементами інформації про захист.

1). *Захист сегментів імен файлів*. Захист сегментів імен файлів запобігає призначення операторами імен файлів, ідентичних іменам, що генеруються програмним забезпеченням. Тим самим забезпечується збереження процесів, що використовують фіксовані імена файлів.

2). *Атрибути захисту файлів*. До атрибутів захисту файлів відносяться:

- дозволи на доступ. Дозволами на доступ визначається, чи дозволено виконання наступних операцій з файлом: зміна імені файлу, зміна періоду зберігання, видалення, читання, запис;

- кількість потрібних резервних копій. Число потрібних резервних копій визначає кількість копій, які повинні бути записані на магнітну стрічку або передані у віддалений комп'ютер до того, як користувачеві буде дозволено: видалити локальний дисковий файл; звільнити область копіювання циклічного файлу; відкрити локальний диск для перезапису;

- період зберігання. Період зберігання - це інтервал часу, протягом якого дисковий файл залишається захищеним після того, як процес "зняв" захист, який реалізують дозволами на доступ. Протягом періоду зберігання забезпечується захист файла від: перейменування; видалення; перезапису;

- прапорець передач. Прапорець передачі вказує, чи був файл успішно скопійований принаймні один раз.

3). *Псевдоніми.* Псевдоніми - це додаткові імена для системних файлів, що зберігаються на магнітному диску. У порівнянні з системними іменами файлів вони мають такі переваги:

- вони можуть бути в будь-який час змінені;

- ці ім’я призначаються відповідно до правил, прийнятих в компанії-оператора, а не встановленими в системі;

- забезпечується додатковий захист під час сеансу *FTAM*-передачі.

Сеанс *FTAM*-передачі може бути ініційований віддаленим процесором тільки шляхом зазначення псевдоніма. Якщо файлу не призначений псевдонім, то він не може бути переданий в режимі *FTAM* з використанням системного імені файлу.

Захист файлів, пов’язаних з ініціаторами. Повноваження на доступ до файлу реєструються для кожного ініціатора. Це забезпечує відхилення запитів на доступ до файлів, що надходять від несанкціонованих ініціаторів. Адміністрування бази даних для системи захисту файлів, пов'язаної з ініціаторами, може виконуватися за *Q*3-запитами.

У разі класичної конфігурації *EWSD* пов’язана з ініціаторами, захист файлів може використовуватися в якості альтернативи, захист групи файлів за допомогою паролів. Однак необхідна процедура повинна бути обрана під час інсталяції.

Пов’язаний з ініціаторами захист файлів може використовуватися при зверненні до всіх зовнішніх діалогів або до сеансів передачі файлів.

Захист файлів, пов'язаних з паролями. Захист файлів, пов'язаний з паролями, реалізується в основному за допомогою пароля для групи файлів, але він підтримується також при використанні захисту файлів, пов'язаної з ініціаторами.

Для отримання доступу до файлів, захищених за допомогою пароля, необхідно передати пароль.

Виведення аварійних звітів. Зокрема, виводиться звіт про порушення прав доступу.

Інформація про всі порушення захисту файлів оформляється у вигляді звітів про порушення прав доступу. Звіти про порушення прав доступу є повідомлення, які можуть бути передані і збережені в пам'яті системи.

3.2.6 Захист під час передачі файлів

Засоби захисту під час передачі файлів складаються з таких компонентів:

- захист доступу до системи;
- захист доступу до даних;
- перевірка спостережності (тільки для *FTAM*);
- висновок аварійних звітів.

Захист доступу до системи. Розрізняють локальні сеанси передачі даних, що запускаються в координаційному процесорі системи *EWSD*, і сеанси, що запускаються в віддаленому процесорі-партнері.

Локально ініційований сеанс передачі даних можна запустити тільки в рамках діалогового сеансу *MML*, керування яким виконується механізмами забезпечення захисту *MML*. (див. розділ 3.2.2).

У разі дистанційного ініціювання передачі даних спочатку виконується ідентифікація процесора-партнера на основі його мережевого адресу. Потім виконується ідентифікація і аутентифікація користувача з використанням ідентифікатора користувача та пароля, що передаються з мережевою адресою.

В інтерфейсі передачі файлів можуть використовуватися наступні механізми аутентифікації:

- механізм захисту за допомогою простих паролів користувача;

- механізм захисту за допомогою простих паролів ідентифікують користувачів за ідентифікатором ініціатора і аутентіфікують їх з використанням простого пароля;

- механізм захисту за допомогою зашифрованих паролів користувача;

- механізм захисту за допомогою зашифрованих паролів ідентифікують за ідентифікатором ініціатора і аутентифікує їх з використанням зашифрованого паролю.

Захист доступу до даних. Для сеансів передачі файлів застосовуються всі механізми захисту файлів, описані в розділі 3.2.6.

Передача файлів можлива тільки в тому випадку, якщо ініціатор має ідентифікатор з повноваженнями на виконання команд передачі даних для локально ініційованих сеансів передачі (див. розділ 3.2.1).

Перевірка спостережності (тільки для FTAM). Вихідні повідомлення, автоматично видаються застосуванням передачі даних *FTAM* для всіх успішно реалізованих сеансів передачі (початок і закінчення), записуються в файл хронології. Кожен запис містить наступні дані:

- дата і час;
- код користувача;
- ім’я процесора-партнера;
- *FTAM*-дані.

На основі цієї інформації завжди можна визначити, які файли запрошувалися, від якого процесора надійшов запит, який використовувався код користувача і куди були передані файли.

Висновок аварійних звітів. Контролюються наступні порушення правил доступу:

- введення невідомих ідентифікаторів користувачів у відповідності з описом в розділі 3.2.3;

- введення невірних паролів користувача у відповідності з описом в розділі 3.2.3;

- несанкціоновані сеанси передачі файлів

Повторні спроби запуску сеансу передачі файлів, незважаючи на недостатні права на виконання команди, призводять до блокування ідентифікатора користувача в разі досягнення порогового значення.

3.3 *IP*-захист в мережах *TCP/IP*

Для забезпечення захисту функціонування *EWSD* через *TCP/IP* використовується функція "захисту *internet*-протоколу" (*IPSEC*).

IPSEC забезпечує захист з'єднань між мережними вузлами *EWSD* і *NetManager* (або іншими операційними системами, що підтримують цю функцію). Для трактів передачі із захистом за допомогою *IPSEC* в якості параметрів використовуються наступні дані:

1. *IP*-адреси (мережевих вузлів, системи *NetManager*);

2. Режим протоколу: аутентифікаційний заголовок (*AH)* та/або інкапсулююче захисне корисне навантаження (*ESP*);

3. Використовуються методи шифрування;

4. Криптографічні ключі (для кожного режиму протоколу і захищеного тракту передачі).

Адміністрування *IPSEC*-з’єднань здійснюється за допомогою програми "*IP Security Administration*" ("Адміністрування *IP*-захисту") системи *NetManager*. При

використанні цього застосування може виконуватися реєстрація або модифікація параметрів, а також перевірка цих параметрів на несуперечність. Крім того, за допомогою цього застосування виконується розподіл параметрів у мережі передачі даних та їх активізація.

Запитання для самоконтролю

1. На які категорії поділяються функції забезпечення захисту у вузлах EWSD?
2. З яких компонентів складаються механізми забезпечення захисту *EWSD*?
3. Яким чином забезпечується захист доступу до системи в мережевому вузлі EWSD?
4. Що таке класи повноважень і з якою метою вони встановлюються?
5. Яким чином працює перевірка спостережності? Для чого необхідна така функціональність?
6. Наведіть порушення правил доступу, за якими здійснюється контроль за граничними значеннями. Хто конфігурує ці граничні значення?
7. Яким чином здійснюється функція управління доступом до Q3?
8. Що таке журнал контролю захисту? Для чого він портрібен?
9. З яких компонентів складаються засоби захисту файлів? Дайте стислий опис цих компонентів.
10. За допомогою чого здійснюється захист у мережах TCP/IP?

4 ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ПРОГРАМНО-КЕРОВАНИХ АТС

Далі у цьому розділі розглядається конкретний приклад організації робіт з технічного захисту інформації в ЦАТС типу EWSD.

4.1 Розробка плану захисту цифрової АТС

4.1.1 Загальні положення

План захисту інформації на ЦАТС визначає зміст робіт відповідно до вимог НД ТЗІ 1.4-001-2000 „Типове положення про службу захисту інформації в автоматизованій системі”.

План захисту розробляється на підставі проведеного аналізу технології обробки інформації, аналізу ризиків, сформульованих тимчасових положень політики безпеки інформації.

Безпека інформації – це стан стійкості інформації до випадкових та зловмисних дій, що виключає недопустимі ризики її знищення, спотворення та розкриття, які можуть привести матеріальні втрати власнику або користувачу інформації.

Цифрова АТС класифікується згідно НД ТЗІ 2.5-003.99 як автоматизована система класу “3” – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

4.1.2 Мета захисту

1. Захист на ЦАТС конфіденційної інформації, яка їй належить, чи якою вона розпоряджається, а саме це відомості, які є власністю власника станції, пов’язані з технологічною інформацією, управлінням, фінансами, наданням послуг та іншою діяльністю ЦАТС, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам.
2. Захист інформації з обмеженим доступом, що є власністю держави.
3. Захист відомостей, які складають комерційну, особисту та інші види таємниць, які підлягають захисту.
4. Захист відкритої інформації, важливої для особи, суспільства і держави, яка зберігається та циркулює в ЦКС.

4.1.3 Основні завдання захисту

1. Забезпечення визначених політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації ЦАТС.
2. Своєчасне виявлення та знешкодження загроз ресурсам ЦАТС, причин та умов, які можуть привести до порушення її функціонування та розвитку.
3. Створення механізму та умов оперативного реагування на загрози безпеці інформації, інші прояви негативних тенденцій у функціонуванні ЦАТС.
4. Ефективне попередження загроз ресурсам ЦАТС на основі комплексного впровадження правових, морально-етичних, фізичних, організаційних, технічних та інших заходів забезпечення безпеки.

3. Управління засобами захисту інформації, управління доступом користувачів до ресурсів ЦАТС, контроль за їх роботою з боку персоналу служби захисту інформації, оперативне сповіщення про спроби несанкціонованого доступу до ресурсів ЦАТС .

6. Реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації.

7. Створення умов для максимально можливого відшкодування та локалізації збитків, що наносяться несанкціонованими діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками, зменшення негативного впливу наслідків порушення безпеки на функціонування ЦАТС .

4.1.4 Основні об'єкти захисту:

1. Відомості, віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється на ЦАТС і які можуть знаходитись на паперових, магнітних, оптичних та ін. носіях.

2. Інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси.

3. Обладнання вузла комутації та інші матеріальні ресурси, включаючи технічні засоби та системи, які не обробляють ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки. Технічні області, в яких необхідно захищати інформаційне та програмне забезпечення – робоча станція, фізична мережа та комутаційне обладнання.

4. Засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту.

3. Користувачі ЦАТС.

4.1.5 Загрози інформації в ЦАТС

Опис загроз інформації в ЦАТС наведено у розд. 2.1.3 та 2.2.

4.1.6 Політика безпеки інформації на ЦАТС

Політика безпеки (ПБ) інформації ЦАТС базується на таких документах:

- Закон України „Про захист інформації в автоматизованих системах" від 03.07.94 р.;

- НД ТЗІ 1.1-001-99 „Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення".

Під політикою безпеки інформації розуміється набір вимог, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Політика безпеки визначає інформаційні ресурси, які потребують захисту, та категорії інформації.

Формуються загрози для ЦАТС, персоналу, інформації різних категорій та вимоги до захисту від цих загроз. ПБ включає в себе вимоги до забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється.

Політика безпеки визначає такі аспекти забезпечення захищеності інформаційних ресурсів у технологічному середовищі АТС:

- гарантії безпеки середовища персоналу;
- гарантії стандартизації технологічного середовища;
- гарантії забезпечення спостереження й керованості технологічного середовища;
- гарантії забезпечення конфіденційності і цілісності інформаційних ресурсів технологічного середовища;
- гарантії якості документації.

Нормальне функціонування АТС на всіх стадіях її життєвого циклу забезпечує персонал, тому необхідно забезпечити захищеність інформаційних ресурсів від їх помилкових і зловмисних дій.

Вимоги до персоналу включають у себе:

- вимоги до системи організації праці – забезпечення відповідності кваліфікації персоналу складу виконуваних робіт, система підвищення кваліфікації тощо;
- вимоги до контролю системи організації праці – контроль кваліфікації персоналу, аналіз і контроль системи підвищення кваліфікації, аналіз системи підбору кадрів, аналіз розподілу повноважень, аналіз системи оцінки якості праці тощо;
- вимоги до поведінки персоналу в робочий час – підтримання загальної дисципліни праці, виконання правил роботи з секретною інформацією та інше;
- вимоги до контролю поведінки персоналу в робочий час – контроль виконання технологічної дисципліни і поведінка персоналу у робочий час тощо;
- вимоги до поведінки персоналу в неробочий час – відсутність фактів антигромадської діяльності, аномалій у психофізичному стані організму і таке інше;
- вимоги до контролю поведінки персоналу у неробочий час – контроль достовірності даних про персонал, перевірка стану здоров’я персоналу.

Для забезпечення гарантій якості стандартизації технологічного середовища необхідно виконати вимоги: до повноти обхвату нормативними документами (НД) елементів середовища, до повного обхвату НД елементів технологій роботи в середовищі та до рівня відповідності НД.

Забезпечення спостережності та керованості технологічного середовища залежить від виконання вимог: до ефективності аудиту технологічного середовища, до аутентифікації суб’єктів та ідентифікації об’єктів (процесів, ресурсів), до сертифікованих шляхів керованості технологічним середовищем.

Вимоги до забезпечення конфіденційності та цілісності інформаційних ресурсів технологічного середовища включають в себе: вимоги до реалізації правил розмежування доступу (ПРД), до реалізації послуг повторного використання об’єктів, до захищеності від таємних каналів витоку та каналів спеціального впливу на елементи АТС, до фізичної цілісності, розмежування обов’язків та самотестуванню об’єктів.

Для забезпечення гарантій якості документації необхідно виконати вимоги: до повноти документації, до рівня деталізації опису середовища та/або технології, достовірності інформації в документації, до якості оформлення документації.

Політика безпеки має бути завершена планом захисту інформації, у якому відображаються основні вимоги і положення інформаційної безпеки.

4.1.7 Календарний план робіт із захисту інформації на ЦАТС

На підставі НД ТЗІ 1.4-001-2000 „Типове положення про службу захисту інформації в автоматизованій системі” складається календарний план робіт із захисту інформації на ЦАТС.

Він може мати такі розділи:

- організаційні заходи;
- контрольно-правові заходи;
- профілактичні заходи;
- робота з кадрами;
- інженерно-технічні заходи.

Організаційні заходи захисту інформації – це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне розв’язання задач захисту шляхом регламентації діяльності персоналу і порядку функціонування систем забезпечення інформаційної діяльності та засобів забезпечення ТЗІ.

До контрольно-правових заходів можуть бути віднесені:

- контроль за виконанням персоналом (користувачами) вимог, відповідних інструкцій, розпоряджень, наказів;
- контроль за виконанням заходів, розроблених за результатами попередніх перевірок;
- контроль за станом зберігання та обігу носіїв інформації на робочих місцях.

До профілактичних слід відносити заходи, спрямовані на формування у персоналу та користувачів мотивів поведінки, які спонукають їх до безумовного виконання у повному обсязі вимог режиму, правил проведення робіт тощо.

Планування роботи з кадрами включає заходи з підбору та навчання персоналу і користувачів встановленим правилам безпеки інформації, новим методам захисту, підвищення їхньої кваліфікації.

До інженерно-технічних слід відносити заходи, спрямовані на налагодження, випробовування і введення в експлуатацію, супроводження й технічне обслуговування апаратних і програмних засобів захисту інформації від НСД, комплексів захисту інформації від загроз технічними каналами та каналами спеціального впливу, інженерного обладнання споруд і приміщень, в яких розміщуються засоби обробки інформації тощо.

Політика безпеки та комплексний план її реалізації є основою для побудови та функціонування системи безпеки.

4.2 Розробка заходів захисту від витоку інформації технічними каналами

Збереження інформаційних ресурсів АТС визначається умовами забезпечення їх захищеності на станції та в мережі. Для рішення цієї задачі розробляється система безпеки, основними функціями якої є захист інформації при її обробці та передачі каналами зв'язку від НСД до неї, від різноманітних програмно-технічних впливів, а також від витоку технічними каналами за рахунок побічних електромагнітних випромінювань та наводок (ПЕМВН).

4.2.1 Оцінка долі технічних каналів витоку у загальній безпеці

В АТС основна увага приділяється питанням захисту інформації від НСД. Заходи захисту інформації від ПЕМВН зустрічаються рідко і застосовуються у особливо відповідальних випадках. Це пояснюється тим, що здійснення різних видів НСД, як всередині ЦАТС, так і зовні з мереж, не потребує великих витрат, оскільки виконується з використанням штатних технічних засобів самих ЦАТС. Ймовірність атак за рахунок НСД в АТС дуже висока. Організація перехоплення інформаційних сигналів каналами ПЕМВН потребує високих витрат, так як пов'язана з використанням спеціальних комплексів перехвату. Крім того, проведення таких атак можливе лише при умові розташування апаратури перехоплення в безпосередній близькості від об'єкта, у відношенні до якого проводиться атака.

Але недооцінка загроз витоку інформації каналами ПЕМВН призводить до того, що вони можуть стати самим вразливим місцем в системі інформаційної безпеки.

4.2.2 Організація захисту інформації від витоку за рахунок ПЕМВН

Захист інформації від витоку за рахунок ПЕМВН повинен бути реалізований або у всій ЦАТС, або в тих сегментах, де обробляється найбільш важлива інформація. Такого захисту на ЦАТС, в першу чергу, потребують приміщення центру технічної експлуатації, оскільки там обробляється технологічна інформація. В загальному випадку всередині контрольованої зони АТС можуть бути виділені внутрішні зони безпеки, в яких повинен бути реалізований захист від ПЕМВН.

Рівні ПЕМВН залежать від параметрів (амплітуди, форми, тактової частоти) сигналів, які обробляються, а також від конструктивного виконання обладнання. Ці ж фактори визначають характер затухання випромінювань з відстанню та радіус зони-2 (мінімально необхідної контрольованої зони) навколо обладнання. Найбільш потужні випромінювання ідуть від моніторів ПЕОМ, а також фізичними лініями. Інші технічні засоби ЦАТС утворюють більш низькі рівні випромінювання. Окрім випромінювань канали витоку виникають в результаті електромагнітних наводок на кола, які виходять за межі контрольованої зони (електроживлення та заземлення, охоронна та пожарна сигналізації) та інших факторів.

Як правило, на ЦАТС більшу частину каналів ПЕМВН намагаються закрити організаційно-технічними рішеннями. Проблему випромінювань фізичних ліній можна зняти використанням криптографічного захисту чи використанням ВОЛЗ. Системи електроживлення, заземлення та сигналізації можна розмістити у контрольованій зоні. Використання таких заходів знижує ймовірність витоку, але не вирішує повністю проблеми ПЕМВН, так як залишаються випромінювання моніторів та фізичних ліній (на неохоплених захистом ділянках), і необхідно використовувати додаткові заходи захисту.

В загальному випадку потрібно вибрати комплекс технічних засобів захисту. При цьому необхідно враховувати ряд загальних вимог, які пред'являють до такого комплексу: ефективність, економічність, відповідність основним характеристикам систем, надійність і т. д.

Комплекс може включати активні та пасивні технічні міри захисту. Активні заходи полягають у маскуванні (зашумленні) побічних випромінювань та наводок поблизу технічних засобів широкосмугових шумових сигналів, які перевищують за рівнем сигнали ПЕМВН. До них відносяться, в основному, генератори шуму. Пасивні заходи захисту спрямовані на ослаблення побічних випромінювань та наводок. До них відносяться екранування, фільтрація, схемно-конструктивна доробка та ін. Які саме заходи потрібно реалізувати, в кожному конкретному випадку розглядається окремо.

Незалежно від того, які засоби захисту будуть прийняті, потрібно правильно розрахувати радіус зони-2, який характеризує мінімальну відстань від технічного засобу, на границі та за межами якого відношення сигнал/шум не перевищує нормованого значення.

4.2.3 Розрахунок границь ближньої та дальньої зони при вимірах ПЕМВ

Для вибору належного рівня захисту технічних засобів обробки інформації необхідно виміряти рівень побічних електромагнітних випромінювань та розрахувати радіус зони-2, на границі та за межами якої відношення сигнал/шум не перевищить нормованого значення. В загальному випадку ця відстань може знаходитись в ближній, перехідній чи дальній зоні. В межах кожної з зон згасання електромагнітної хвилі описується різними аналітичними залежностями. Уміння вірно визначити границі зон необхідне для одержання об'єктивної оцінки величини зони-2.

В даний час границі зон визначаються умовно без достатнього математичного або електродинамічного обґрунтування. Таким чином, при розрахунку радіусу зони-2 допускаються методичні погрішності, що неприпустимо при організації захисту інформації обмеженого поширення від витоку за рахунок ПЕМВ. Для багатьох технічних засобів обробки інформації, наприклад персональних ЕОМ, характерна велика величина амплітуди напруги небезпечного сигналу і мала величина амплітуди струму. Такі джерела відносять до електричних випромінювачів.

Будемо вважати ПЕОМ точковим електричним випромінювачем, тому що його розміри істотно менші відстані до точки можливого перехоплення інформації. Представимо його у вигляді диполя, розміщеного в точці О сферичної системи координат.

Математичні вирази для визначення параметрів поля джерела ПЕМВ можна одержати з класичної теорії технічної електродинаміки, використовуючи вирази для векторного потенціалу. Відомо, що вектори напруженості магнітного H та електричного E полів пов'язані з векторним потенціалом залежностями:

$$H = (1/\mu) rotA_a \ , \quad E = (1/i\varpi\varepsilon_a\mu_a) rotrotA_a ,$$

де ε_a - абсолютна комплексна діелектрична проникність; $A_a = \mu_a Ile^{-ikr}/(4\pi r)$; μ_a - абсолютна магнітна проникність середовища; I - струм в провіднику; l - довжина провідника; r - відстань від випромінювача до вимірювальної антени (точки спостереження); k - хвильове число.

Розкладемо векторний потенціал на радіальну (A_r), кутову (A_θ) та азимутальну (A_φ) складові:

$$A_r = \frac{\mu_a}{4\pi} Il \frac{e^{-ikr}}{r}\cos\theta , \quad A_\theta = -\frac{\mu_a}{4\pi} Il \frac{e^{-ikr}}{r}\sin\theta \ , \quad A_\varphi = 0 .$$

В сферичній системі координат складові вектора напруженості електричного поля описуються наступними виразами:

$$E_r = -i\frac{Il}{2\pi\varpi\varepsilon_a} e^{-ikr}\left(\frac{1}{r^3} + \frac{ik}{r^2}\right)\cos\theta \ , \tag{4.1}$$

$$E_\theta = -i\frac{Il}{4\pi\varpi\varepsilon_a} e^{-ikr}\left(\frac{1}{r^3} + \frac{ik}{r^2} - \frac{k^2}{r}\right)\sin\theta \ , \tag{4.2}$$

$$E_\varphi = 0 .$$

Вектор напруженості електричного поля має вигляд $E = rE_r + \theta E_\theta$. Силові лінії вектора E проходять у меридіальних площинах. Складова E_θ досягає максимального значення при $\theta = \pi/2$ в екваторіальній площині та рівна нулю на осі диполя. Тому вимірювання ПЕМВ потрібно здійснювати в напрямі максимального випромінювання ПЕОМ при $\theta = \pi/2$. Складова E_r пропорційна $\cos\theta$ та досягає максимуму на осі диполя, а в екваторіальній площині рівна нулю.

З урахуванням хвильового опору середовища без втрат $\rho_0 = (\mu_a/\varepsilon_a)^{1/2}$, швидкості поширення $v_0 = (\mu_a/\varepsilon_a)^{-1/2}$ та довжини хвилі $\lambda = v/f$, вираз (4.2) для E_θ можна представити у вигляді:

$$E_\theta = \rho_0 Il\left[\frac{1}{4\pi r^2} - i\left(\frac{\lambda}{8\pi^2 r^3} - \frac{1}{2\lambda r}\right)e^{-ikr}\right]. \tag{4.3}$$

При вимірюванні напруженості електричної складової поля за допомогою селективних мікровольтметрів використовується режим пікового або квазі-пікового детектування. В цьому випадку амплітуда напруженості електричної складової поля може бути виражена наступним чином:

$$E_m = \sqrt{(E_{m1} - E_{m3})^2 + E_{m2}^2} \ , \tag{4.4}$$

де $E_{m1} = \rho_0 \frac{Il\lambda}{8\pi^2}\frac{1}{r^3}$, $E_{m2} = \rho_0 \frac{Il}{4\pi}\frac{1}{r^2}$, $E_{m3} = \rho_0 \frac{Il}{2\lambda}\frac{1}{r}$.

Простір навколо випромінювача умовно розділяється на 3 зони – ближню, перехідну та дальню. Характер залежності амплітуди електричної складової від дальності залежить від того, в якій зоні знаходиться точка спостереження.

Розглянемо залежності амплітуди електричної складової в ближній, перехідній та дальній зонах.

Ближня зона. Під ближньою зоною розуміється область навколо випромінювача, для якої $|kr| << 1$, де $k = 2\pi / \lambda$ - хвильове число. Відповідно, $r << \lambda/(2\pi)$. Враховуючи, що $|kr| << 1$, приймемо $|kr| = 0$. В цьому випадку вирази (4.1) та (4.2) можна привести до виду:

$$E_r = -i\frac{Il}{2\pi\varpi\varepsilon_a}\frac{1}{r^3}\cos\theta, \quad E_\theta = -i\frac{Il}{4\pi\varpi\varepsilon_a}\frac{1}{r^2}\sin\theta. \tag{4.5}$$

Дальня зона. Під дальньою зоною розуміється область простору навколо випромінювача, для якої $|kr| >> 1$ чи $r >> \lambda/(2\pi)$. Нехтуючи доданками з більш високими степенями r в знаменнику, отримуємо:

$$E_\theta = i\frac{k^2 Il}{4\pi\varpi\varepsilon_a}\frac{e^{-ikr}}{r}\sin\theta. \tag{4.6}$$

Перехідна зона. Під перехідною зоною розуміється область простору навколо випромінювача, в якому відстань r від випромінювача до вимірювальної антени порівняно з довжиною хвилі λ. Це значить, що жодним з доданків в (4.3) нехтувати неможна. В даній зоні формула для розрахунку електричної складової поля має вигляд:

$$E_\theta = A\sqrt{\left[\left(\frac{\lambda}{4\pi^2 r^3} - \frac{1}{\lambda r}\right)^2 + \left(\frac{1}{2\pi r^2}\right)^2\right]}, \tag{4.7}$$

де $A = \rho_0 Il/2$ - енергетичний коефіцієнт.

Взаємне порівняння внеску кожної зі складових в амплітуду напруженості електричного поля дозволяє визначити границі зон з достатньою для практики точністю.

Відстанню до границі ближньої зони $r_{бл}$ назвемо відстань від джерела ПЕМВ, на якій максимальна складова E_{m1} у ξ раз перевищує внесок складової E_{m2}. У межах даної відстані можна зневажити складовими E_{m2} і E_{m3} і вважати, що результуюча амплітуда електричної складової поля дорівнює складовій E_{m1}.

З рівняння $E_{m1} = \xi E_{m2}$ можна одержати шуканий вираз до границі ближньої зони $r_{áëèç} = \lambda/(2\pi\xi)$. Аналогічно, для границі дальньої зони отримуємо $r_{äàë} = \xi\lambda/(2\pi)$.

Величина прийнятого граничного внеску складових поля ξ залежить від необхідної точності і для практичних розрахунків може складати величину від 3 до 10. На границі ближньої (дальньої) зони можна обмежитися значенням ξ=3, при якому у виразі (4.4), з урахуванням зведення членів у квадрат, величинами E_{m2} і E_{m3} (E_{m1} і E_{m2}) можна зневажити в порівнянні з E_{m1} (E_{m3}). Так, для ξ=3 границя ближньої зони складає $r_{áëèç} = \lambda/(6\pi)$, а границя дальньої зони - $r_{äàë} = 3\lambda/(2\pi)$.

Ширина перехідної зони залежить від довжини хвилі ПЕМВ та обраної точності розрахунків і дорівнює $D = \lambda(\xi^2 - 1)/(2\pi\xi)$. При $\xi \geq 3$ ширину перехідної зони можна визначити виразом $D \approx \xi\lambda/(2\pi)$. Таким чином, на фіксованій частоті

ширина перехідної зони залежить тільки від обраної точності розрахунків. У граничному випадку при великих значеннях ξ ширина смуги необмежено зростає, що приводить до необхідності враховувати всі члени у виразі (4.4) незалежно від відстані до джерела ПЕМВ.

Розрахуємо радіус зони-2 у випадку, коли ПЕМВ є персональна ЕОМ. Середня частота роботи монітора 110 МГц. Звідси маємо, що довжина хвилі становить:

$$\lambda = \frac{3\times10^8}{110\times10^6} = 2{,}73 \ м.$$

Тоді границя ближньої зони становить:

$$r_{áë} = \frac{2{,}73}{6\times3{,}14} = 0{,}15 \ м.$$

Границя дальньої зони

$$r_{ä} = \frac{3\times2{,}73}{2\times3{,}14} = 1{,}30 \ м.$$

Ширина перехідної зони

$$D = \frac{2{,}73\times(3^2-1)}{2\times3\times3{,}14} = 1{,}15 \ м.$$

Як видно з розрахунків, границя дальньої зони при частоті монітора 110 МГц становить 1,30м. Віддалення границь від джерела ПЕМВ визначається довжиною хвилі та зі збільшенням частоти переміщується в сторону джерела. Тому при виборі ПЕОМ для робочого місця оператора з точки зору системи технічного захисту потрібно вибирати монітори з якнайменшою робочою частотою, аби радіус зони, на границі та за межами якої відношення сигнал/шум не перевищить нормованого значення, те ж був мінімальним.

4.3 Організація та реалізація системи захисту системи сигналізації *SS*7

4.3.1 Структура та організація системи сигналізації SS7

Система спільноканальної сигналізації (*SS*7) служить для передачі інформації між ЦАТС (АМТС) з програмним управлінням. *SS*7 використовується для інформаційного обміну сигнальною інформацією в процесі встановлення з'єднання, управління процесами встановлення з'єднання, маршрутизацією та трафіком, організації інтеграції та надання послуг, контролю, технічної діагностики, технічного обслуговування, конфігурації та реконфігурації мережі, її агрегатних засобів та інших застосувань. У відповідності з цим „Національна версія України" передбачає в *SS*7:

- підсистему передачі повідомлень (*MTP – Message Transfer Part*);
- підсистему управління з'єднанням сигналізації (*SCCP – Signaling Connection Control Part*);
- підсистему користувача цифрової мережі з інтеграцією послуг (*ISUP – ISDN User Part*);
- підсистему використання можливостей транзакції;
- підсистему експлуатації та технічного обслуговування *SS*7;
- підсистему користувача технічної експлуатації мережі зв'язку.

Основною властивістю *SS*7 є те, що один канал (16-ий часовий інтервал 30-канальних цифрових з'єднувальних ліній) використовується для переносу повідомлень сигналізації, які відносяться до кількох розмовних каналів. Також цей канал використовується для переносу повідомлень управління розмовними каналами та управління мережею сигналізації. Мітка, яка присутня в кожному сигнальному повідомленні, використовується для однозначного визначення розмовного каналу, до якого відноситься дане повідомлення.

Система *SS*7 забезпечує надійну та достовірну передачу сигнальної інформації як наземними, так і супутниковими каналами зв'язку. Вона може застосовуватись на міжнародній, міжміській, внутрішньо зоновій та місцевих мережах.

Система *SS*7 ТМЗК України може працювати у двох режимах: спільному та квазіспільному, що дозволяє будувати мережу сигналізації з високим використанням ланок. За спільного режиму роботи для кожного маршруту робочих каналів відводяться сигнальні канали *SS*7 у тому ж маршруті.

За квазіспільного режиму роботи маршрут проходження інформації сигналізації на комутаційній ділянці може не співпадати з розмовними каналами. В цьому випадку маршрут *SS*7 проходить через один або кілька транзитних пунктів сигналізації (ТПнС).

При передаванні інформації *SS*7 основним маршрутом використовується спільний режим роботи. При передачі інформації *SS*7 обхідними маршрутами можуть використовуватись спільний або квазіспільний режим роботи.

*SS*7 ТМЗК України організується на базі стандартних цифрових каналів зі швидкістю 64 кбіт/с. Сигнали каналами *SS*7 передаються методом послідовної передачі по ділянках (ланках сигналізації), з однієї ділянки на іншу, після їх обробки у пунктах сигналізації (ПнС) або ТПнС.

Підсистема передачі повідомлень (*MTP*) утворена трьома функціональними рівнями:

- перший рівень визначає фізичні, електричні та функціональні характеристики ланки даних сигналізації та засоби доступу до неї. Елемент першого рівня є каналом зв'язку для ланки сигналізації;

- другий рівень визначає функції та процедури, що належать до передачі сигнальних повідомлень окремою ланкою даних сигналізації. Із сигнальних повідомлень, які надходять з верхніх рівнів, на другому рівні формуються сигнальні одиниці, які мають, окрім сигнальної інформації, ще і інформацію для управління передачею. Перший та другий рівні утворюють ланку сигналізації.

- третій рівень вміщує в себе функції та процедури обміну сигнальними повідомленнями між вузлами мережі сигналізації (пунктами сигналізації), які зв'язані ланками сигналізації. Ці функції діляться на дві категорії:

- обробка повідомлень сигналізації;

- управління мережею сигналізації.

Четвертий рівень є набором підсистем користувачів, в кожній з яких реалізовані функції, які характерні для користувачів даної підсистеми.

Одним з основних користувачів є підсистема користувача цифрової мережі з інтеграцією послуг (*ISUP*). На цьому рівні обробляються сигнальні

повідомлення, які управляють телефонними з'єднаннями у відповідності з міткою маршрутизації та інформацією користувача.

Мережа сигналізації може бути поділена на рівні з метою оптимального адміністрування.

Специфікація *SS*7 дозволяє поділити мережу на ієрархічні рівні, які відповідають традиційному принципу побудови телефонної мережі: міжнародний, національний та місцевий (регіональний) (рис. 4.1).

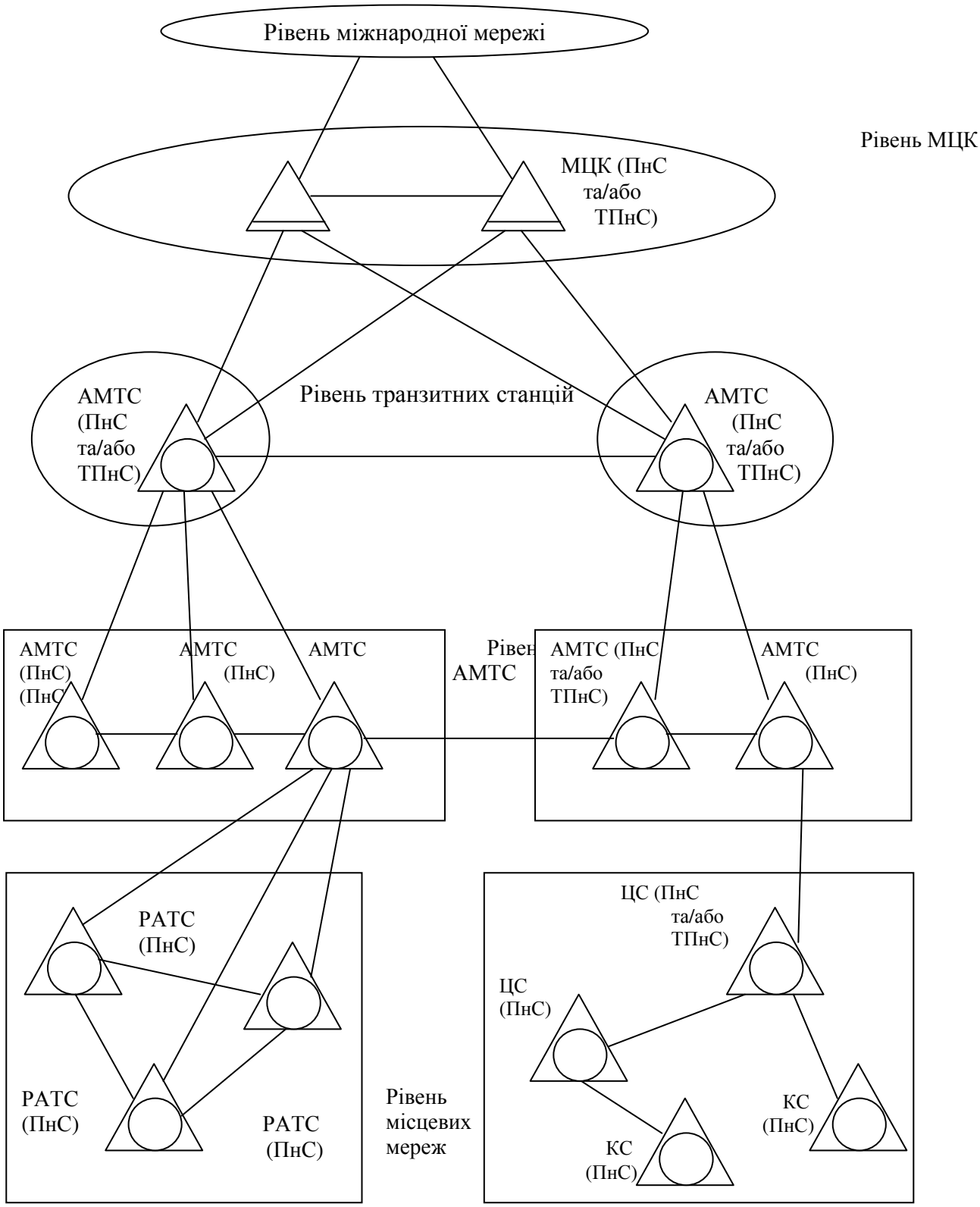

Рисунок 4.1 – Схема багаторівневої мережі *SS*7

При використанні системи *SS*7, в процесі установлення і з'єднання розмовний тракт не перевіряється, тому що лінійні сигнали ним не передаються. Щоб виключити можливість передачі абонентам зіпсованого розмовного тракту, у системі може передбачатися шлейфна перевірка розмовних каналів. Шлейфна перевірка полягає у підключенні до тракту приймально-передавального пристрою на вихідній станції та організації шлейфа на вхідній станції. Перевірка повинна проводитися за ділянками.

Нумерація пунктів сигналізації всередині кожного рівня – незалежна, значення мережного індикатора визначає до якої мережі відноситься дане повідомлення.

Основними перевагами *SS*7 є:

- швидкість – у більшості час встановлення з'єднання менше 1 сек.;
- один канал сигналізації здатний одночасно керувати 2-4 тисячами розмовних каналів;
- економність – у порівнянні з іншими системами сигналізації зменшує кількість обладнання на ЦАТС;
- гнучкість – система передає будь-які дані, не лише дані телефонії, але й дані цифрових систем з інтеграцією служб, мереж рухомого зв'язку, інтелектуальних мереж тощо;
- надійність – досягається за рахунок можливості альтернативної маршрутизації у мережі сигналізації.

У період створення та становлення мереж *SS*7 проблеми захисту інформації від різноманітних загроз були не такі актуальні. Головна увага приділялась питанням забезпечення надійності мережі та достовірності передачі даних мережею (цілісності даних та цілісності мережі). Захищеність даних від несанкціонованого втручання виявилась порівняно низькою.

4.3.2 Система захисту у мережі *SS*7

Спочатку мережа *SS*7 створювалася в припущенні, що невелика кількість магістральних мереж будуть взаємодіяти з обмеженою кількістю місцевих, і дані будуть передаватися в замкнутому середовищі – між комутаторами і базами даних (БД) – з мінімальним втручанням людини. У такому випадку вважалося, що всі дані надходять з надійних джерел. Тому протоколи *SS*7 на відміну від *IP*-протоколів не підтримують функції шифрування й аутентифікації. Акцент у ТфМЗК було зроблено на захисті обладнання, а не протоколів.

Відносно принципів роботи мережі сигналізації були прийняті наступні заходи безпеки. Шлюз у складі транзитного пункту сигналізації маршрутизатора мережі *SS*7 виконує сканування повідомлень, що надходять у мережу, щоб запобігти надходженню повідомлень з неавторизованих внутрішніх і зовнішніх вузлів мережі.

Оскільки зараз зв'язок розвивається дуже швидко, мережа *SS*7 використовується в широкому діапазоні застосувань і тому більше не є закритою мережею. Доступ до неї має велика кількість користувачів інших

мереж. Кожна точка взаємодії мереж різних типів – це потенційна загроза безпеки.

Як уже говорилося вище, мережі сигналізації не підтримують функції шифрування й аутентифікації, за допомогою яких можна гарантувати достовірність вузлів зовнішньої мережі, що посилають повідомлення.

Наприклад, сервер, що посилає спеціальні руйнуючі повідомлення, може порушити роботу сигнальної мережі і перервати обслуговування клієнтів. Елементи самої мережі сигналізації також не захищені. Якщо зловмисник зможе відправити на деякий вузол мережі *SS*7 трафік, що перевищує той, на який цей вузол розрахований, останній вийде з ладу, і управління викликами в цьому секторі мережі буде порушено.

Сучасні підходи до захисту мережі *SS*7 припускають надання їй додаткових інтелектуальних властивостей. Спеціальні програми, установлені на транзитних пунктах, дозволяють операторам ідентифікувати повідомлення, що випадають із загального контексту або виявляють себе нетиповим поводженням.

Одним з важливих способів підвищення безпеки мережі є побудова правильної архітектури на стику ТфМЗК – *IP*-мережі. Кількість вузлів з'єднання цих мереж повинне бути мінімальним, повідомлення з мережі *SS*7 повинні надходити на *IP*-шлюзи централізовано. Замість численних шлюзів використовується єдиний високопродуктивний шлюз. Тоді за рахунок скорочення точок взаємодії між різнорідними частинами мережі підвищується загальна безпека мережі.

Ще одне питання захисту мережі *SS*7 пов'язане з тим, що на сучасних мережах широко використовується централізована обробка і управління мережею *SS*7. У зв'язку з цим використовуються спеціальні функції, розроблені для дистанційного експлуатаційного управління АТС, заміни версії програмного забезпечення тощо. Вони також являють собою загрозу інформаційної безпеки, тому що дані функції можуть збігатися з цілями зловмисника. У зв'язку з цим для процедур вилученого доступу необхідно моніторинг міжстанційної і міжмережної інформації, захист від загрози пересилання по мережі сигналізації спеціальних директив шляхом їх фільтрування при вході у фрагмент мережі, що захищається.

Як правило, доступ до спеціальних функцій АТС, створюваних виробником, реалізується за допомогою не задокументованої адреси джерела і спрямовано до інструментів експлуатаційного управління ЦАТС. Наведемо деякі не задокументовані функції:

- функція завантаження/розвантаження станційної БД. Така утиліта дозволяє завантажувати у виробника і досліджувати БД на предмет її функціонування, а також завантажувати нову БД. Існування утиліти може дозволити зловмисникові вивантажити БД системи, модифікувати її або вставити програмну закладку;
- функція перевірки/модифікації станційної БД. Утиліта дозволяє дистанційно досліджувати і модифікувати БД системи для усунення несправностей через неправильну конфігурацію, помилки конструкції тощо. Ця

утиліта дає можливість модифікувати БД для одержання доступу до спеціальних функцій;

- функція наладчика/відновлення ПЗ. Така утиліта дозволяє дистанційно налагоджувати несправну систему в умовах, у яких вона не справно працює. Функція також дає можливість дистанційно обновляти системи з виявленими дефектами. Це місце найбільш вразливе, тому що доступ зловмисника до ПЗ дає практично необмежений доступ до ЦАТС і мережі.

Описані загрози можна вважати первинними або безпосередніми через розуміння загрози не тільки як деякої потенційної небезпеки, що наносить збиток інформаційній системі, але і як безпосередньому впливові на АТС, *SS*7 і на мережу в цілому. Нормальна робота мережі багато в чому також залежить від навантаження, створюваного на мережі *SS*7, тому таке навантаження необхідно контролювати.

4.4 Розрахунок надійності системи управління ЦАТС

Обробка технологічної інформації на ЦАТС, її зберігання та контроль за роботою системи в цілому проводиться оператором за допомогою персональної ЕОМ. Оскільки повна чи часткова втрата цієї інформації може привести до порушення роботи ЦАТС, збоїв в системі, то важливо знати, наскільки надійним є обладнання, яке використовується оператором при роботі.

Стандартом (ГОСТ 13377-75) дається таке визначення терміну *надійність* – це властивість об'єкта виконувати задані функції, збереження у часі значень встановлених експлуатаційних показників у заданих межах, які відповідають заданим режимам та умовам використання, технічного обслуговування, ремонтів, зберігання й транспортування.

Кількісною оцінкою надійності найчастіше є ймовірність безвідмовної роботи, тобто ймовірність того, що при роботі у заданих умовах система буде задовільно виконувати необхідні функції протягом встановленого проміжку часу. Така модель справедлива при умовах:

- допущення, що надійність має ймовірнісний характер за можливості появи відмовлення;
- система працює задовільно за повільного погіршення її параметрів у часі;
- система працює у незмінних умовах навколишнього середовища.

Ймовірність є величина безрозмірна, яка може приймати значення у інтервалі від 0 до 1. Якщо функції системи і критерії відмовлення точно задані, то надійність може бути точно виражена кількісно через ймовірності.

При розрахунку надійності, в залежності від призначення обладнання, на перший план висувається її безвідмовність, довговічність чи ремонтопридатність.

Безвідмовність – це властивість пристрою безперервно зберігати працездатність.

Довговічність – це властивість заданий строк зберігати працездатність до руйнування або іншого граничного стану.

Ремонтопридатність – це можливість ремонту та технічного обслуговування обладнання.

Виходячи з цього, під *надійністю* розуміють властивість апаратури, обумовлену її безвідмовністю, довговічністю та ремонтопридатністю за умови виконання заданих функцій, тобто це здатність виконувати визначені задачі у визначених умовах експлуатації.

Велике значення в теорії та практиці надійності має поняття відмовлення. Під *відмовленням* розуміють подію, яка полягає в порушенні працездатності пристрою.

Оскільки відмовлення є випадковою подією, то для визначення надійності обладнання використовуються ймовірнісні характеристики – ймовірності відмовлення та безвідмовної роботи.

Ймовірністю безвідмовної роботи називається ймовірність того, що в заданому інтервалі часу t при заданих режимах і умовах роботи не відбудеться жодного відмовлення. Час t безвідмовної роботи приладу є випадковою величиною із середнім значенням T_m. Ймовірність безвідмовної роботи визначається з виразу:

$$P(t) = p(T_m \geq t), \tag{4.8}$$

де $p(T_m \geq t)$ - ймовірність того, що відмовлення не відбудеться протягом часу t, який не перевищує значення T_m.

При розрахунках ймовірності безвідмовної роботи використовується наступна формула:

$$P(t) = e^{-\lambda t}, \tag{4.9}$$

де λ - інтенсивність відмовлень.

Ймовірністю відмовлення $Q(t)$ називається ймовірність того, що в даному інтервалі часу відбудеться хоча б одне відмовлення:

$$Q(t) = q(T_m < t), \tag{4.10}$$

де $q(T_m < t)$ - ймовірність того, що відмовлення відбудеться в інтервалі часу t.

Оскільки несправна та безвідмовна робота є протилежними несумісними подіями, то справедлива наступна рівність:

$$Q(t) = 1 - P(t). \tag{4.11}$$

Інтенсивністю відмовлень $\lambda(t)$ називається ймовірність відмовлень не відновлюваного пристрою в одиницю часу після даного моменту часу t за умови, що до цього моменту відмовлення не виникло. Кількісно інтенсивність відмовлень виражається в числі відмовлень, що приходяться на одну годину роботи.

Наробітком на відмовлення називається середнє значення часу роботи T_m відновлюваного елемента між відмовленнями і визначається за формулою:

$$T_m = \frac{1}{\lambda}. \tag{4.12}$$

При розрахунку ймовірності безвідмовної роботи пристрою інтенсивність відмовлень цього пристрою визначається за формулою:

$$\lambda = \sum_{i=1}^{n} \lambda_i \ , \qquad (4.13)$$

де n – кількість видів елементів, що складають необхідний пристрій;

λ_i – загальна інтенсивність відмовлень елементів одного виду.

Розрахуємо надійність обладнання на робочому місці оператора центру технічної експлуатації. Для цього в табл. 4.1 приведемо дані про елементи, що складають ПЕОМ – їх кількість та інтенсивність відмовлень.

Розрахуємо за формулою (4.13) сумарну інтенсивність відмовлень ПЕОМ:

$$\lambda = \lambda_{мон} + \lambda_{мп} + \lambda_{в} + \lambda_{д} + \lambda_{сд} + \lambda_{з} + \lambda_{пр} + \lambda_{кл} + \lambda_{м} + \lambda_{зк} = = (2{,}6 + 3{,}5 + 0{,}2 + 0{,}19 + 0{,}19 + 3 + 0{,}2 + 9{,}09 + 0{,}25 + 0{,}075) \times 10^{-6} = = 19{,}295 \times 10^{-6} \ 1/ч.$$

Тепер за формулою (4.12) розрахуємо середній час наробітку на відмовлення:

$$T_m = \frac{1}{\lambda} = \frac{1}{19.295 \times 10^{-6}} = 51826{,}8 \text{ години.}$$

Як видно, середній час наробітку на відмовлення ПЕОМ з даною інтенсивністю відмовлень дорівнює 51826,8 години, що складає майже 6 років.

Таблиця 4.1 – Інтенсивність відмовлень елементів персональної ЕОМ

Найменування елемента	Кількість елементів одного виду в ПЕОМ, n	Інтенсивність відмовлень одного елемента, $\lambda_э * 10^{-6}$, 1/год	Сумарна інтенсивність відмовлень елементів одного виду, $n * \lambda_э * 10^{-6}$, 1/год
Монітор	1	2,6	2,6
Системний блок: - материнська плата	1	3,5	3,5
- вінчестер	1	0,2	0,2
- дисковод 3’5”	1	0,19	0,19
- флеш-пам’ять	1	0,14	0,14
- CD-ROM	1	0,19	0,19
- звукова плата	1	3	3
Прінтер	1	0,2	0,2
Клавіатура (клавіші)	101	0,09	9,09
Мишка	1	0,25	0,25
З’єднувальний кабель	5	0,015	0,075

Це не означає, що ПЕОМ виходить із ладу через кожні шість років. Це означає, що у великій партії ПЕОМ, кожна з них має випадковий час наробітку на відмовлення T_i.

Якщо знайти середнє значення часу наробітку на відмовлення ПЕОМ даної партії, тобто знайти суму наробітків на відмову кожної з ПЕОМ і поділити цю суму на кількість ПЕОМ у партії, то одержимо вказані значення T_m. Якщо процеси виникнення відмов мають властивість ергодичності, тоді середнє за ансамблем (тобто середнє значення T_i за всією партією) можна замінити середнім за часом. Тобто можна спостерігати довгий час за одним комп'ютером.

Щоб показати це наглядно, розрахуємо за формулою (4.9) ймовірність безвідмовної роботи ПЕОМ протягом цих шести років. Результати цього розрахунку зведемо в табл. 4.2. Фізичний смисл даних цієї таблиці полягає у тому, що за час роботи ПЕОМ - t ймовірність її безвідмовної роботи складає величину $P(t)$.

За результатами табл. 4.2 побудуємо графік залежності ймовірності безвідмовної роботи від часу (рис. 4.2).

Таблиця 4.2 – Ймовірності безвідмовної роботи ПЕОМ у залежності від часу

Час роботи t, ч	Ймовірність безвідмовної роботи, $P(t)$
0	1
10000	0.8245
20000	0.6798
30000	0.5605
40000	0.4622
50000	0.381
60000	0.346

Для побудови графіка зручно зв'язати рисунок як об'єкт з Exel.

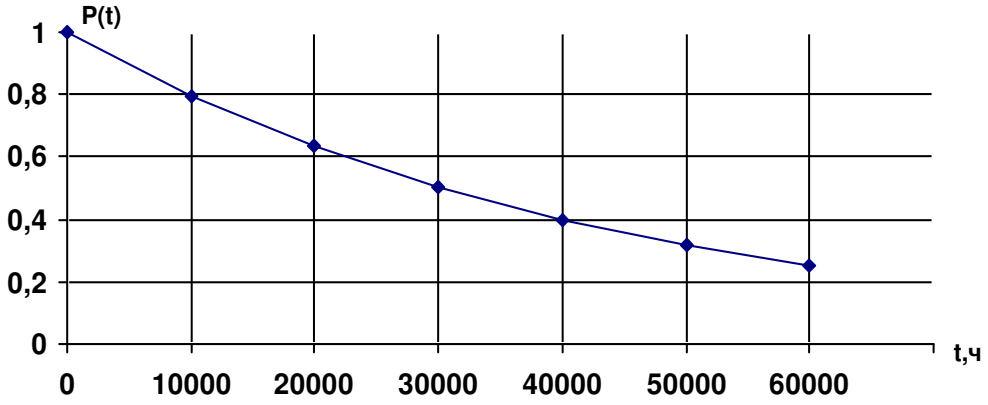

Рисунок 4.2 – Графік залежності ймовірності безвідмовної роботи ПЕОМ у залежності від часу роботи

Як видно з графіка, ймовірність безвідмовної роботи ПЕОМ за 60000 годин падає практично до нуля. А це значить, що для того, щоб попередити

пошкодження чи втрату технологічної інформації на ЦАТС внаслідок виходу з ладу ПЕОМ на робочому місці оператора, під кінець цього строку комп'ютер бажано замінити на новий.

Наведена методика розрахунку надійності можна застосовувати для широкого кола технічних пристроїв.

4.5 Рекомендації з обмеження фізичного доступу до устаткування зв'язку в абонентській мережі

Метод обмеження фізичного доступу до устаткування зв'язку спрямовано на те, щоб унеможливити для зловмисника фізичне сприйняття інформативних сигналів, які існують у лінії зв'язку, колах апаратури та навколишньому просторі. Для досягнення такої мети слід застосовувати апаратуру, перевірену на відсутність упроваджених «закладок», пломбувати експлуатовану апаратуру, ремонт апаратури робити лише з залученням довірених фахівців під контролем власника чи співробітника служби безпеки підприємства.

Необхідно виключити будь-які ініціативні переробки впровадженої до експлуатації апаратури обслуговуючим персоналом чи ремонтниками. Особливу увагу слід звертати на легко замінювані елементи. Наприклад, кабель, що з'єднує телефонний апарат з апаратом захисту (скремблером, шифратором), може бути замінено за кілька секунд, а його конструкція й габарити припускають установлення закладки. Такі елементи слід додатково закріплювати й маркувати. Додаткове кріплення й маркування повинні бути непомітні для стороннього спостерігача, але легко перевірятися власником термінала чи допущеним обслуговуючим персоналом.

Прокладання проводів, які несуть сигнали незахищеної інформації, повинне виконуватися приховано, за можливості без рознімних з'єднань. Функційно необхідні рознімі повинні додатково фіксуватися чи пломбуватися.

Для унеможливлення перехоплення інформації з електромагнітних полів бажано застосовувати сертифіковану апаратуру, виконуючи вказівки щодо її розміщення. За використання іншої апаратури бажано провести інструментальну перевірку можливості приймання сигналів захищеної інформації у безпосередній близькості (10....15 см) від апаратури.

Кола, що відходять, повинні бути максимально віддалені від апаратури опрацьовування інформації. Кабелі, шнури, що несуть сигнал захищеної інформації, повинні бути екрановані. Оскільки застосування сертифікованої апаратури й рекомендоване розташування апаратури та кабелів в умовах комерційного підприємства часто є нездійсненні, корисним може бути розташування в складі абонентського термінала генераторів електромагнітного шуму. При цьому випромінювальні системи (антени) генераторів повинні бути максимально сполучені в просторі з випромінювальними елементами апаратури. У цілому при організації робочого місця абонента захищеного Зв'язку слід дотримувати правил:

- на робочому місці має бути мінімум апаратури й устаткування;
- встановлення всього устаткування та елементів інтер'єра має утруднювати їхнє переміщення й заміну чи впровадження сторонніх предметів;

- на випадок, якщо відбудуться порушення розташування, заміна чи впровадження нового предмета, тоді слід вжити заходів задля виявлення й знешкодження певних дій;

- повинно бути максимально утруднене для зловмисника спостерігання за робочим процесом зв'язку й ознайомлення з системою та апаратурою захисту інформації.

Слід зазначити, що за всієї простоти пропонованих заходів, їхня реалізація й, головне, оцінювання ефективності потребують глибокого аналізу конкретної апаратури зв'язку, її розташування й приміщення, в якому встановлено термінал. Це пов'язано з тим, що більшість процесів, які призводять до витоку інформації (за винятком безпосереднього приєднання зловмисника до лінії зв'язку), мають паразитний характер, не нормуються документацією на апаратуру, не виявляються в головному робочому процесі. Багато параметрів цих процесів істотно змінюються від екземпляра до екземпляра апаратури зв'язку і сполучених з нею виробів, істотно залежать від впливів, що не впливають на головний робочий процес (наприклад від переміщення кабелів електроживлення).

Оцінювання значущості тих чи інших паразитних процесів у конкретній ситуації, вибір раціональних заходів щодо придушення, формування правил експлуатації термінала в частині підтримування на необхідному рівні його інформаційної захищеності вимагають високої кваліфікації й якісно можуть бути виконані лише із залученням спеціалізованої організації.

Запитання для самоконтролю

1. Дайте визначення поняття «комплекс засобів і механізмів захисту». Чим КЗМЗ відрізняється від КСЗІ?

2. Що називають моделлю захисту?

3. Поясніть схему структури забезпечення технічного захисту інформації у ЦКС.

4. Наведіть номенклатуру штатних функціональних послуг захисту (ФПЗ), які складають функції захисту.

3. Які п'ять аспектів забезпечення захищеності інформації в технологічному середовищі створення та експлуатації систем ТЗІ включає у себе система гарантій?

6. Дайте характеристику інформації, яка підлягає захисту у цифрових АТС загального користування.

7. Яким загрозам інформаційним ресурсам цифрової АТС має протидіяти КСЗІ?

8. З чого складається штатний комплекс засобів та механізмів захисту ЦАТС?

9. Поясніть систему позначень штатних ФПЗ за допомогою термів.

10. Що називають «слабким місцем у захисті»?

11. Що називають «виломом захисту»?

12. Дайте приклад комплексу заходів для нейтралізації «слабкого місця».

13. Дайте коротку характеристику загальних засобів захисту, які реалізуються у кожній системі захисту.

14. Якими є мета і зміст плану захисту інформації в ЦАТС?

13. Що розуміють під політикою безпеки інформації?

16. Прокоментуйте вимоги до персоналу ЦАТС.

17. Наведіть зміст календарного плану робіт із захисту інформації на ЦАТС.

18. Як організовано захист інформації від витоку технічними каналами за рахунок ПЕМВН?

20. Поясніть призначення, загальну структуру та організацію системи сигналізації *SS7*.

21. Яка система захисту у мережі *SS7*?

22. Який порядок розрахунку надійності об’єктів ЦАТС, які складаються з багатьох об’єктів?

23. Що називають надійністю об’єкта?

24. Що є кількісною оцінкою надійності об’єкта?

23. Який фізичний смисл поняття середній час наробітку на відмовлення та як він обчислюється?

5 ОЦІНКА ВЕЛИЧИНИ ВИТРАТ НА СИСТЕМУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОГРАМНО-КЕРОВАНИХ АТС

Загальним принципом діяльності у сфері захисту інформаційних ресурсів є максимум ефективності за допустимого ризику інформаційної безпеки не нижчого від зафіксованого, коли оперативний ризик є мінімальним, забезпечення єдності економічних, технічних та організаційних методів, оцінних критеріїв та засобів визначення достовірності оцінки рівня інформаційної безпеки для підвищення ефективності діяльності підприємства.

Важливою та необхідною складовою роботи з впровадження КСЗІ ЦАТС є уміння розраховувати та економічно обґрунтовувати розмір необхідних вкладень у забезпечення безпеки в рамках єдиної стратегії безпеки на основі аналізу ризиків, порівняння витрат на забезпечення інформаційної безпеки з потенційними збитками та ймовірністю їх виникнення.

Неоціниму допомогу у написанні цього розділу, створенні методик оцінки витрат на інформаційну безпеку ЦАТС та проведенні розрахунків було надано кандидатом економічних наук Т.М. Тардаскіною, за що автор виявляє їй свою вдячність.

5.1 Загальна структура витрат на інформаційну безпеку

Система інформаційної безпеки ЦКС може бути ефективною, якщо витрати на її створення та управління будуть принаймні менші за втрати внаслідок знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку маршрутизації інформації.

Необхідний рівень безпеки можна визначити при наявності:

- системи показників для оцінки ефективності підсистеми безпеки і методики їхнього виміру;
- посадових осіб, уповноважених приймати рішення про допустимість визначеного рівня залишкового ризику;
- системи, що дозволяє відслідковувати поточні параметри підсистеми безпеки.

Витрати на інформаційну безпеку поділяються за наступними категоріями:

- витрати на технічне обслуговування системи захисту інформації і заходи щодо запобігання порушень політики безпеки підприємства (витрати на попереджувальні заходи);
- витрати на формування і підтримування ланки керування системою захисту інформації (організаційні витрати);
- витрати на контроль, тобто на визначення і підтвердження досягнутого рівня захищеності ресурсів на ЦАТС;
- внутрішні витрати на ліквідацію наслідків порушення політики інформаційної безпеки – це витрати, понесені підприємством зв’язку, у результаті того, що необхідний рівень захищеності не був досягнутий;
- зовнішні витрати на ліквідацію наслідків порушення політики інформаційної безпеки – це компенсація втрат при порушенні політики безпеки

у випадках, пов’язаних з витоком інформації, втратою іміджу, утратою довіри партнерів і абонентів тощо.

Розглянемо детальніше структуру витрат за кожною категорією.

А. Витрати на обслуговування системи безпеки (витрати на попереджувальні заходи):

1) керування системою захисту інформації:

- витрати на планування системи захисту інформації підприємства;
- витрати на вивчення інформаційної інфраструктури підприємства із забезпечення безпеки інформації обмеженого поширення;
- витрати на здійснення технічної підтримки виробничого персоналу при впровадженні засобів захисту, процедур і планів із захисту інформації;
- перевірка співробітників на лояльність (вірність), виявлення загроз безпеки;
- організація системи допуску виконавців і співробітників конфіденційного діловодства з відповідними штатами й оргтехнікою;

2) регламентне обслуговування засобів захисту інформації:

- витрати, пов’язані і настроюванням програмно-технічних засобів захисту, операційних систем і використаного мережного устаткування;
- витрати на організацію мережної взаємодії і безпечного використання ЦАТС;
- витрати на підтримку системи резервного копіювання і ведення архіву даних;
- проведення інженерно-технічних робіт із установлення сигналізації, устаткуванню сховищ конфіденційних документів, захисту телефонних ліній зв’язку, засобів обчислювальної техніки тощо;

3) аудит системи безпеки:

- витрати на контроль змін стану інформаційного середовища підприємства;
- витрати на систему контролю за діями виконавців;

4) якість технологій:

- витрати на забезпечення відповідності вимогам якості інформаційних технологій, у тому числі аналіз можливих негативних аспектів інформаційних технологій, що впливають на цілісність і доступність інформації;
- витрати на доставку (обмін) конфіденційної інформації;
- задоволення суб’єктивних вимог користувачів: стиль, зручність інтерфейсів тощо;

5) довіра до технології: витрати на забезпечення відповідності прийнятим стандартам і вимогам, вірогідності інформації, дієвості засобів захисту;

6) навчання персоналу:

- підвищення кваліфікації співробітників підприємства в питаннях використання наявних засобів захисту, виявлення і запобігання загроз безпеки;
- розвиток нормативної бази служби безпеки;

7) витрати на заробітну плату секретарів і службовців, організаційні та інші витрати, що безпосередньо пов'язані з попереджувальними заходами.

Б. Витрати на контроль:

1) планові перевірки і випробування:

- витрати на перевірки і випробування програмно-технічних засобів захисту інформації;
- витрати на перевірку навичок експлуатації засобів захисту персоналом підприємства;
- витрати на забезпечення роботи осіб, відповідальних за реалізацію конкретних процедур безпеки по підрозділах;
- оплата робіт з контролю правильності введення даних у прикладні системи;
- оплата інспекторів із контролю вимог, запропонованих до захисних засобів при розробці будь-яких систем (контроль виконується на стадії проектування та специфікації вимог);

2) позапланові перевірки й іспити:

- оплата роботи експертів спеціалізованих організацій;
- забезпечення експертів (внутрішніх і зовнішніх) матеріально-технічними засобами;

3) дотримання політики безпеки:

- витрати на контроль реалізації функцій, що забезпечують керування захистом комерційної таємниці;
- витрати на організацію тимчасової взаємодії і координації між підрозділами для вирішення повсякденних конкретних задач;
- витрати на проведення аудиту безпеки по кожній автоматизованій інформаційній системі, виділеної в інформаційному середовищі підприємства;
- матеріально-технічне забезпечення системи контролю доступу до об'єктів і ресурсів підприємства;

4) зовнішні контрольні витрати на контрольно-перевірочні заходи, пов'язані з ліцензійно-дозвільною діяльністю в сфері захисту інформації;

5) аналіз політики безпеки підприємства:

- витрати на ідентифікацію загроз безпеки;
- витрати на пошук вразливостей системи захисту інформації;
- оплата роботи фахівців з визначення можливого збитку й переоцінці ступеня ризику.

В. Внутрішні витрати на ліквідацію наслідків порушення політики безпеки:

1) відновлення системи безпеки до відповідності вимогам політики безпеки:

- придбання останніх версій програмних засобів захисту інформації;
- придбання технічних засобів замість тих, що прийшли у непридатність;
- проведення додаткових іспитів і перевірок технологічних засобів;
- витрати на утилізацію скомпрометованих ресурсів;

2) відновлення інформаційних ресурсів підприємства у разі порушення інформаційної безпеки:

- витрати на відновлення баз даних і інших інформаційних масивів;

- витрати на проведення заходів щодо контролю вірогідності даних, які підверглися атаці на цілісність;

3) витрати на виявлення причин порушення політики безпеки:

- витрати на проведення розслідувань порушень політики безпеки (збір даних про способи здійснення, механізми і способи приховання неправомірного діяння: пошук слідів, знарядь і предметів зазіхання; виявлення мотивів неправомірних дій тощо);

- витрати на відновлення планів забезпечення безперервності діяльності служби безпеки;

4) витрати на доробки системи інформаційної безпеки:

- витрати на впровадження додаткових засобів захисту, що вимагають істотної перебудови системи безпеки;

- витрати на повторні перевірки й іспити системи захисту інформації.

Г. Зовнішні витрати на ліквідацію наслідків порушення політики безпеки:

1) зобов'язання перед державою і партнерами (відновлення довіри):

- витрати, притягнуті для відновлення довіри споживача, партнерів і держави;

- витрати на юридичні суперечки і виплати компенсацій;

- втрати в результаті розриву ділових відносин з партнерами;

2) втрата новаторства:

- витрати на проведення досліджень і розробки нової ринкової стратегії;

- відмовлення від організаційних, науково-технічних чи комерційних рішень, що стали неефективними в результаті витоку зведень, і витрати на розробку нових засобів ведення конкурентної боротьби;

- втрати від зниження пріоритету в наукових дослідженнях і неможливості патентування та продажу ліцензій на науково-технічні досягнення;

3) виникнення труднощів у просуванні продукції, у придбанні чи устаткування технологій, у тому числі підвищення цін на них;

4) економічний збиток:

- інші види можливого збитку підприємству, у тому числі зв'язані з неможливістю виконання функціональних задач, визначених його Статутом.

Для реальної системи інформаційної безпеки склад і структура витрат може бути іншою у залежності від задач, які система вирішує.

5.2 Методи кількісних, якісних та експертних оцінок параметрів інформаційної безпеки

Оцінка рівня захищеності інформаційних ресурсів, ефективності механізмів захисту та загальної захищеності систем, економічних показників та інших параметрів системи забезпечення інформаційної безпеки телекомунікаційних мереж та їх складових є вельми складною задачею. На сьогодні визнані фахівцями методики оцінки поки що відсутні.

Справа ускладнюється тим, що не всі показники рівня захищеності інформаційних ресурсів мають кількісні оцінки. Дійсно, оцінка захищеності

інформації від витоку її технічними чи фізичними каналами (акустичними, віброакустичними, електричними, електромагнітними, оптичними тощо) виконується порівнянням відповідного виміряного рівня сигналу з нормою. Якщо відношення рівня сигналу, виміряного на границі чи за межами контрольованої зони, до рівня, прийнятого за норму, менше «1», то об'єкт вважається захищеним.

Але за несанкціонованого доступу до інформації у комп'ютерній системі не вдається знайти фізичну величину, яку при цьому можна виміряти. Доводиться застосовувати якісні оцінки захищеності.

5.2.1 Експертні методи оцінки параметрів інформаційної безпеки

Показники, які залежать від антропогенних впливів, здебільшого мають якісні оцінки у порядкових шкалах, здобутих методом експертного опитування. Показники захищеності являють собою систему взаємозв'язаних і взаємозалежних компонентів. Оцінка степені захищеності окремих телекомунікаційних об'єктів – вузлів, станцій, маршрутизаторів, серверів – є складною задачею, яка виконується експертами.

Дослідження у області експертних систем показали ефективність застосування для вирішення таких задач інтелектуальних систем підтримки прийняття рішень, заснованих на експертних знаннях. Об'єктивні оцінки захищеності мереж замінюються експертними оцінками, основаними на евристичних наданнях переваг. Робота експертних систем заснована на знаннях, які зберігаються у пам'яті системи.

Для подання знань у експертній системі підтримки прийняття рішень із оцінки варіантів розподілу механізмів інформаційної безпеки з використанням нечіткої логіки та нечітких множин, можна запропонувати мережну конструкцію, яка задається у вигляді

$$C = <X_{11},\ldots, X_{ij}; R_1,\ldots, R_k; G> \qquad (5.1)$$

де X – множина об'єктів телекомунікаційної мережі (вузлів, каналів) потужністю i, в кожному з об'єктів якої виділяються $j = 9$ модулів безпеки (три площини безпеки по три рівня в кожній площині. Див. розд. 11.3);

$R_1,\ldots, R_i$ – множина типів зв'язків між об'єктами;

G – відображення, яке задає зв'язки між об'єктами X із заданого набору зв'язків.

Відповідна експертна система подається у вигляді трьох взаємопов'язаних моделей: об'єктної моделі, яка відображає дані щодо структурних аспектів мережі; динамічної моделі, яка описує роботу об'єктів мережі; функціональної моделі, у якій розглядається взаємодія між об'єктами (рис. 5.1).

База знань експертної системи складається з теоретичного матеріалу з проблем побудови телекомунікаційних мереж та КСЗІР в ній, а також специфічної експертної інформації, необхідної для підтримки прийняття рішень.

Прийняття рішень щодо раціонального вибору варіантів і оцінки захищеності мереж виконується за допомогою правил вирішення. Кожне

правило базується на інформації, отримуваної від експерта. За допомогою правил вирішення проводиться часткове впорядкування (ранжирування) точок простору вхідних показників.

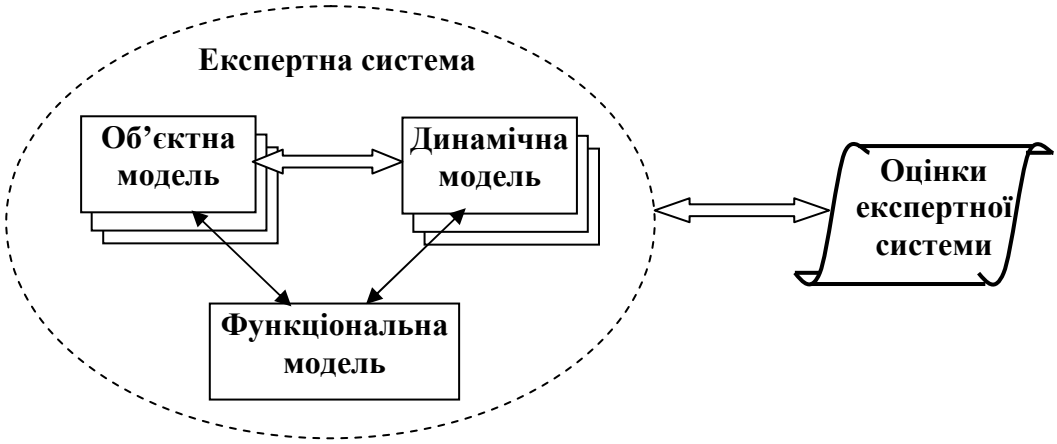

Рисунок 5.1 – Структура експертної системи

Для оцінки степені захищеності мереж *методами нечіткої логіки та нечітких множин вводяться лінгвістичні змінні*:

r – степінь захищеності інформаційного ресурсу, яка забезпечується механізмом інформаційної безпеки у модулі безпеки компонента мережі;

s – степінь ризику (ймовірність) здійснення загрози на протязі певного проміжку часу;

p – величина можливих збитків, які можуть бути нанесені оператору внаслідок реалізації загроз.

Для оцінки ймовірності загрози вводяться декілька дискретних степенів (градацій). Лінгвістичні змінні приймають терм-множину значень T_p, T_r і T_s відповідно

$$T_p = T_r = T_s = \{\text{“незначна”, “низька”, “середня”, “висока”}\}. \quad (5.2)$$

Границі між значеннями змінних розмиті. Функції приналежності різних термів пересікаються. Значення змінних у кожному конкретному випадку визначається експертним методом або емпіричним шляхом, на основі досвіду експлуатації подібних систем, шляхом реєстрації певних подій, визначення частоти їх повторення тощо. Величина можливих збитків визначається розміром фінансових втрат або, у випадку неможливості їхнього визначення, за якісною шкалою. Наприклад, величина збитків може бути - “відсутня”, “низька”, “середня”, “висока”, “недопустимо висока”.

Дослідження степені захищеності мереж проводять за правилами, які формуються на основі експертного опитування. Основна ідея цього методу полягає у наступному: експертні оцінки задаються у вигляді рівнянь призначення – нечітких відношень, які містять обмеження на базові змінні. Вхідні нечіткі інструкції можуть бути подані деякою комбінацією вхідних правил. Ці рівняння вирішуються відносно бажаних обмежень за допомогою композиції нечітких відношень.

Економічна частина цільових функцій має задаватись виходячи з того принципу розумної достатності, згідно якого витрати на інформаційну безпеку $B_{ІБ}$ мають бути менші за можливі збитки $B_З$ за реалізації загроз: $B_{ІБ} < B_З$. Нечітку базу даних представляють у вигляді:

$$\bigcup_{l=1}^{k_j}[\bigcap_{i=1}^{n}(x_i = a_i^{jl})] \to y = d_j;\ j = \overline{1,m};i = \overline{1,n}., \qquad (5.3)$$

де a_i^{jl} – нечіткий терм, яким оцінюється вхід x_i;

вихід y оцінюється нечітким термом d_j;

n – кількість входів;

m – кількість термів, які використовуються для лінгвістичної оцінки вихідних даних; входів;

k – кількість вхідних правил.

Логічне виведення базується на відомому алгоритмі виведення у нечітких експертних системах [19]. У відповідності з алгоритмом база знань подається у вигляді таблиць, де у стовбцях присутні базові значення лінгвістичних змінних r, s, p тощо та їх модифікації, створені логічними зв'язуваннями "і" "або".

З метою використання колективних знань база знань формується шляхом опитування декількох експертів. Для об'єднання індивідуальних суджень у колективне застосовують нечітке відношення "поміж", значення якого подається інтервалом значень на відрізку [0, 1]. Поняття "поміж" у просторі надання переваг є формалізацією умови Парето для принципу узгодження відношень індивідуального надання переваг типу: "якщо всі індивідууми надають перевагу об'єкта a перед об'єктом b, то і у груповому наданні переваг об'єкт a повинен бути кращим об'єкта b".

Процедура побудови правил вирішення повинна бути інтерактивною.

Задача оцінки комплексної системи інформаційної безпеки, розгорнутої на телекомунікаційній мережі є суттєво складною. Така задача є творчою, базується на емпіричному досвіді фахівців, а ефективність результатів визначається наявністю відповідних знань та досвіду фахівців.

При знаходженні оцінки необхідно узгодити між собою низку протилежних принципів, які мають одночасно задовольнятись:

- принцип зменшення потоку інформації, який має доставлятись людині для прийняття рішення;
- принцип об'єктно-орієнтованого моделювання при побудові картини предметної області;
- принцип динамічної структури;
- принцип повноти інформаційного простору;
- принцип інтеграції інформаційного простору;
- принцип децентралізації інформаційного сховища та принцип компонентного складання прикладних режимів.

Рішення експертної системи може бути правильним з деякою ймовірністю. Якщо експертна система має 300 і більше параметрів, вона починає працювати сама на себе [20].

Крім того, один із законів складних систем полягає у тому, що оптимальні показники захищеності ресурсів складної системи можуть досягатись тоді, коли

функціонування механізмів захисту компонентів складної системи не буде оптимальним. Оптимальною величиною захищеності ресурсів системи є така, яка досягається за мінімальних витрат, що мають бути меншими, ніж можливі втрати від реалізації загроз, яким протистоїть КСЗІР.

Оптимальною системою захисту інформації називається така система захисту, яка забезпечує максимальну степінь захищеності при мінімальному потенційному збитку, максимальній функціональності та продуктивності інформаційної системи (максимумі функцій інформаційної системи та мінімумі середнього часу доступу до об'єктів захисту інформаційної системи).

На функціонування механізмів та сервісу інформаційної безпеки витрачаються ресурси телекомунікаційної мережі: час, програмне та апаратне забезпечення, збільшується навантаження мережі та час затримки повідомлень, зменшується пропускна здатність телекомунікаційної мережі. Роль експертної системи прийняття рішень полягає у пошуку компромісу. Механізми інформаційної безпеки повинні нормально функціонувати у кожному модулі безпеки і, при цьому, не заважати роботі інших компонентів КСЗІР телекомунікаційних мереж.

Ще одну проблему складають питання довіри до значень вхідних змінних та коректності бази знань, яка повинна бути побудована на основі експериментально підтверджених матеріалів щодо побудови та функціонування КСЗІР телекомунікаційних мереж.

Необхідно проводити широкі експериментальні дослідження – вести накопичування, документування і використання результатів регулярного моніторингу інформаційної безпеки для вдосконалення і розвитку системи оцінки інформаційної безпеки та одержання статистики технічної експлуатації КСЗІР.

5.2.2 Визначення показників захищеності та побудова матриці показників

При розв'язанні задачі раціонального вибору слід врахувати фактори: на сьогодні не сформовано інтегральної оцінки рівня захищеності, але можливо визначити рівні, що забезпечується кожною конкретною послугою або механізмом безпеки; не всі показники рівня захищеності мають кількісні оцінки, показники, які залежать від антропогенних впливів, здебільшого мають якісні оцінки у порядкових шкалах, одержаних методом експертного опитування.

Показники захищеності, гарантій, якості та взаємозв'язані з ними техніко-економічні показники формуються на різних стадіях життєвого циклу КСЗІР на різних етапах проектування, створення та експлуатації. *Задачі аналізу можна поділити на три класи*:

- детерміновані задачі, коли вихідні дані моделі є повністю визначеними;
- стохастичні задачі, коли у вихідній інформації є елементи невизначеності або деякі параметри носять випадковий характер з відомими ймовірнісними характеристиками, або частина параметрів має якісний характер і оцінюється експертними методами за допомогою якісних шкал та методів нечіткої логіки;

- комбіновані детерміновано-нечіткі задачі, коли у вхідних параметрів присутні, як повністю визначені або стохастичні параметри, наприклад параметри технічних каналів витоку, так і нечіткі параметри, наприклад показники захищеності, які забезпечуються механізмами захисту від несанкціонованого доступу.

При захисті комп'ютерних мереж фізичні та технічні засоби захисту оцінюються детермінованими параметрами. До стохастичних слід віднести різного роду атаки на комп'ютерні мережі: віруси, зломи систем захисту інформації, проникнення в системи тощо. Потік цих подій оцінюється стохастичними параметрами.

Організаційні параметри (засоби) захисту, такі як робота з персоналом, контроль діяльності слід віднести до третього класу, де можливі оцінки якісними або експертними методами. В ТМЗК захист від атак, які носять випадковий характер та захист від людського фактору, є основним.

Показники захищеності являють собою систему взаємозв'язаних і взаємозалежних компонентів; до номенклатури показників, окрім показників захищеності, доцільно залучити показники якості інформаційно-телекомунікаційної системи (такі, як надійність, завадостійкість, показники доставки повідомлень тощо); економічна частина цільових функцій має задаватись виходячи з принципу розумної достатності, що витрати на інформаційну безпеку $B_{ІБ}$ мають бути менші за можливі збитки $B_З$ за реалізації загроз: $B_{ІБ} < B_З$.

Позначимо через $X_1, \ldots, X_n$ набір показників, які відображають показники призначення, захищеність інформації (конфіденційності, цілісності, доступності, спостережності), захищеності системи документальних телекомунікацій (надійності, сталості, живучості), їх якості (достовірності передавання інформації, завадостійкості, характеристик доставки інформації, якості послуг) та гарантії захищеності (відносно всіх етапів життєвого циклу системи). Показник X_n – величина витрат.

Задача оцінки показників захищеності і якості є задачею їх "виміру" й відображення у деякій кількісній або якісній шкалі. Не всі характеристики можуть бути оцінені кількісно, особливо ті, які залежать від антропогенних чинників. Приміром важко оцінити кількісно надійність зв'язку чи якість керування системою безпеки. При неможливості оцінки показника кількісно його оцінюють якісно, відображаючи міру прояву даної прикмети, застосовуючи порядкові шкали і користуючись методом експертного опитування.

Результатом оцінювання повинна бути матриця показників захищеності і якості системи розмірністю $n \times m$, де n – кількість показників, m – кількість варіантів побудови системи інформаційної безпеки. Кожному варіанту відповідає своя точка чи вектор у просторі показників $X_1, \ldots, X_n$, частина з яких є критеріями вибору.

Для прикладу розглянемо три варіанти техніко-економічної задачі раціонального розподілу функціональних послуг захисту з декількома показниками захищеності і якості (табл. 5.1).

Таблиця 5.1 – Матриця показників захищеності та якості телекомунікаційних мереж

Показники захищеності і якості	Оцінки показників для варіантів розподілу послуг забезпечення безпеки і якості системи телекомунікаційних мереж		
	Варіант розподілу між рівнями та прикладною системою	Варіант розподілу між елементами мережі доступу, ЦКС, транспортної мережі	Варіант розміщення послуг у кінцевих пунктах
Достовірності	$p_{П1}$	$p_{П2}$	$p_{П3}$
Надійності	$Н_1$	$Н_2$	$Н_3$
Конфіденційності	$К_1$	$К_2$	$К_3$
Цілісності	$Ц_1$	$Ц_2$	$Ц_3$
Доступності	$Д_1$	$Д_2$	$Д_3$
Спостережності	$С_1$	$С_2$	$С_3$
Вартості	$В_{ІБ}$	$В_{ІБ}$	$В_{ІБ}$
Гарантій захисту	– *Рівень 1*	*Рівень 2*	*Рівень 3*

Економічні показники мають враховувати загальні витрати, включаючи вартість придбання, монтажу (інсталяції) і технічної експлуатації засобу захисту. У варіанті розподілу послуг безпеки між прикладним рівнем і іншими рівнями загальні витрати на інформаційну безпеку можуть бути обчислені за виразом:

$$B_{ІБ1} = \sum_{m=1}^{M} B_m(l_m) + \sum_{i=1}^{I}\sum_{m=1}^{M} B_{im}(l_{im}), \qquad (5.4)$$

де m – індекс механізму безпеки, m=1...M, де M – кількість механізмів безпеки;

$B_m(l_m)$ – величина витрат на реалізацію m-го механізму безпеки з показником захищеності l_m;

i – індекс рівня моделі мережі, i=1...I, де I – кількість рівнів за винятком прикладного рівня;

$B_{im}(l_{im})$ – величина витрат на реалізацію m-го механізму безпеки на рівні i з показником захищеності l_{im}.

У варіанті розподілу послуг безпеки між прикінцевими пунктами і вузлами мережі загальні витрати на інформаційну безпеку $B_{ІБ}$ можуть бути обчислені за виразом

$$B_{ІБ2} = N\sum_{m=1}^{M} B_m(l_m) + V\sum_{j=1}^{J}\sum_{m=1}^{M} B_{jm}(l_{jm}), \qquad (5.5)$$

де N – кількість прикінцевих пунктів;

V – кількість вузлів мережі;

j – індекс блока вузла мережі, j=1...J, де J – кількість блоків на вузлі.

Припустимо, що при переносі засобів захисту з прикінцевого пункту у вузли мережі загальна захищеність не змінюється і не утворюються нові канали несанкціонованого доступу. Тоді з (5.5) випливає, що загальні витрати можуть зменшитись, бо $V < N$. Залежність захищеності від перерозподілу засобів захисту у мережі пов’язана з конкретними параметрами послуг захисту.

5.2.3 Методи вибору оптимального варіанта побудови системи інформаційної безпеки

Методи відбору найбільш раціонального варіанта побудови системи інформаційної безпеки можуть бути такими: диференційний метод; метод багатокритеріального оцінювання; метод комплексного показника; інтерактивний метод.

При *диференційному методі* вибирається базовий аналог, значення показників якого задаються експертом. Оцінюваний варіант признається задовільним, якщо він не поступається аналогу по жодному з показників. У випадку, коли варіант за деякими показниками поступається аналогу а за деякими переважає його, цей метод не застосовується. Диференційний метод зручно застосовувати при первинному відборі варіантів для подальшого аналізу.

Узагальненням диференційного методу є *метод багатокритеріального оцінювання* варіантів за набором показників. У просторі показників задається таке правило порівняння n – мірних точок (вирішне правило): точка x має більшу перевагу, ніж точка y, якщо вона має хоча б одну більшу компоненту і ні однієї меншої. Простір показників поділяється на три області:

X_A - множина точок, кожна з яких має більшу перевагу, ніж будь-яка точка базового варіанта;

X_B - множина точок, кожна з яких не має переваг над базовим варіантом;

X_C - множина точок, кожна з яких має меншу перевагу, ніж хоча б одна точка, яка відповідає базовому варіанта.

При цьому методі необхідна далі більш детальна оцінка відібраних варіантів.

Метод комплексного показника полягає у здобутті згортки показників і до єдиного комплексного показника за формулами, одна з яких може мати вигляд:

$$F = \sum_{i=1}^{n} a_i X_i, \qquad (5.6)$$

де a_i – вагові коефіцієнти, які відображають “важливість” окремих показників.

Цей метод простий, але його неможливо застосувати у нашому випадку, коли показники мають не однакову фізичну природу. Крім того, у комплексному показнику один показник може бути компенсовано іншим. Приміром, занижений показник конфіденційності може компенсуватись завищеним показником продуктивності. Це недопустимо виходячи з принципу “найменш захищеної ланки”.

Більш досконалим є інтерактивний метод вибору раціонального варіанта, який засновано на одній із задач теорії прийняття рішень [21]. Він характеризується використанням експертної інформації не лише для оцінки показників у якісних шкалах, а й для прийняття рішень щодо раціонального вибору. Порівняння багатокритеріальних альтернатив (точок простору показників) виконується за допомогою вирішних правил. Кожне правило базується на інформації, отримуваної від експерта. За допомогою вирішних

правил проводиться часткове впорядкування (ранжирування) точок простору показників.

Задовільність деякого вирішного правила можна з'ясувати лише в процесі його застосування. Тому процедура вибору повинна бути кілька кроковою. Якщо вирішне правило не забезпечує визначеності впорядкування варіантів, то за наступним кроком має бути отримана додаткова інформація і побудоване більш "сильне" вирішне правило, яке дозволило б усунути невизначеність впорядкування варіантів.

Інформацію, отримувану від експерта, необхідно перевіряти на змістовність, адекватність задачі і не суперечливість. Додаткова інформація на кожному кроці повинна порівнюватись із отриманою раніше. Тому процедура побудови вирішного правила повинна бути інтерактивною.

5.2.4 Алгоритм вибору оптимального варіанта побудови системи інформаційної безпеки методом розв'язання задачі багатокритеріального вибору

Таким чином, задачу можна звести до задачі багатокритеріального вибору, яка успішно вирішується у багатьох практичних випадках. Математична постановка задачі така. Задана область параметрів $P(x_1, \ldots, x_m)$ та цільові функції комплексного показника:

$$\begin{aligned} k_1 &= f(x_1,\ldots,x_m), \\ k_2 &= f(x_1,\ldots,x_m), \\ &\ldots \\ k_k &= X_n = f(x_1,\ldots,x_m), \end{aligned} \qquad (5.7)$$

де $k_1,\ldots,k_k$ – вектор критеріїв.

Частину показників вибирають у якості критеріїв, так що $n = m + k$.

Алгоритм процедури пошуку раціонального варіанта розподілу послуг наведено на рис. 5.2.

Спочатку формується загальна стратегія інформаційної безпеки, а на її базі – часткові стратегії варіантів побудови системи захисту. Формуються вимоги до системи захисту і початкове вирішне правило.

В основному циклі процедури формуються варіанти побудови системи інформаційної безпеки на базі інформації експертів. Отримані варіанти ранжуються у просторі критеріїв і застосовується вирішне правило. Далі вилучається найгірший варіант. Якщо таким чином знайдено раціональний варіант, то процедуру закінчено.

В іншому випадку формується інформація для наступної ітерації процедури: деталізуються часткові стратегії, деталізуються вимоги до варіантів і формується "підсилене" вирішне правило. Перевагою цього методу є те, що збирається і аналізується інформація експертів з її ускладненням до наступних циклів. Тим самим уникається надлишковість інформації.

Існуюча парадигма ефективності системи інформаційної безпеки полягає в тому, що величина ризику чи втрат від реалізації загроз має бути меншою ніж витрати на її побудову та керування. Тому мають місце два одночасних процеси.

З одного боку, теорії та нормативно-правова база захисту інформації передбачає оцінку початкового ризику інформаційної безпеки від реалізації загроз та оцінку залишкового ризику після створення системи інформаційної безпеки.

З іншого боку, передбачається побудова системи інформаційної безпеки та обчислення витрат на інформаційну безпеку, враховуючи комплексний підхід для побудови системи забезпечення інформаційної безпеки на всіх стадіях і етапах життєвого циклу, включаючи її створення та експлуатацію.

Рисунок 5.2 – Процедура вибору раціонального варіанта розподілу послуг

5.3 Методика оцінки витрат на забезпечення інформаційної безпеки ЦАТС

Передбачається, що комплексна система захисту інформації цифрової системи комутації створюється згідно з пакетом нормативних документів системи технічного захисту інформації на програмно-керованих АТС загального користування. Цифрові комутаційні системи (ЦКС), як правило, оснащуються штатними і, за необхідності, додатковими позаштатними засобами ТЗІ, які при їхньому спільному використанні утворюють комплекс засобів і механізмів захисту (КЗМЗ), що забезпечує потрібний рівень захищеності інформаційних ресурсів ЦКС.

5.3.1 Структура витрат на інформаційну безпеку ЦАТС

Порядок виконання робіт визначено в [12, 22]. На стадії розробки робочого проекту системи ТЗІ у ЦКС розробляється КЗМЗ, як взаємозв'язаний набір засобів і механізмів захисту, що реалізують обрану модель захисту. Модель захисту розробляється на стадії технічного проектування як взаємозв'язаний набір функціональних послуг захисту з необхідними рівнями ефективності і стійкості реалізації цих послуг, за яких забезпечується заданий у технічному завданні рівень захищеності інформаційних ресурсів.

Штатні засоби і механізми захисту інформації здебільшого вже закладені в архітектуру сучасних ЦКС або в систему їхньої технічної експлуатації. Додаткові засоби і механізми захисту розробляються й застосовуються у випадках, коли штатні не забезпечують необхідного рівня захищеності. Номенклатура штатних ФПЗ та система гарантій наведена в розд. 4.1.

Відповідно до принципу мінімальної достатності система захисту має бути спроектована таким чином, щоб здійснювалася протидія тільки тим загрозам, що мають суттєве значення для Замовника системи ТЗІ, і тільки тою мірою, в якій необхідно нейтралізувати чи послабити, зменшити наслідки прояву таких суттєвих загроз, для того щоб втрати від їхніх можливих реалізацій не перевищили гранично припустимих рівнів. На стадії технічного проектування розробляється модель захисту інформаційних ресурсів ЦКС та визначається сукупність ФПЗ для реалізації КЗМЗ.

Для вперше створюваних ЦКС спочатку виконується вибір системи з огляду на реалізовані у ній ФПЗ таким чином, щоб мінімізувати вартість робіт зі створення додаткових механізмів захисту, якщо в цьому виникає потреба. У сукупності зі штатними додаткові механізми повинні забезпечити зазначений у технічному завданні рівень захищеності інформації. Необхідно вибрати таку систему, штатні засоби захисту котрої найбільш повним чином реалізовували б отриману за результатами технічного проектування модель захисту.

Якщо тип ЦКС вже обрано, то виконується оцінка реалізованих у ній штатних ФПЗ на відповідність, наведеній у технічному проекті моделі захисту. Відсутні послуги реалізуються за допомогою додаткових засобів і механізмів захисту.

На цій стадії можна визначити структуру витрат на інформаційну безпеку, як показано в табл. 5.2. При цьому слід враховувати різницю в життєвих циклах

штатних та додаткових засобів і механізмів захисту, а також їхню часткову реалізацію в існуючій системі технічної експлуатації ЦКС. Частина витрат на інформаційну безпеку на штатні заходи і засоби вже увійшла до вартості системи, що постачається, а також до витрат в системі технічної експлуатації.

Таблиця 5.2 – Структура витрат на інформаційну безпеку в типовій ЦАТС

№ п/п	Підсистема засобів та механізмів захисту інформації	Статті витрат						
		Пошук слабких місць	Проектування	Створення	Оцінка чи тестування	Атестація	Супроводження	Експлуатація
1	Штатні засоби фізичного захисту: укріпленості об'єкта, охорони території, захисту від стихійних лих тощо.	-	-	-	B_{14}	B_{15}	-	-
2	Додаткові засоби фізичного захисту	B_{21}	B_{22}	B_{23}	B_{24}	B_{25}	B_{26}	B_{27}
3	Штатні організаційно-технічні заходи підтримки надійності, архівування, резервування, ремонтоздатності.	-	-	-	B_{34}	B_{35}	-	-
4	Додаткові організаційно-технічні заходи	B_{41}	B_{42}	B_{43}	B_{44}	B_{45}	B_{46}	B_{47}
5	Штатні програмно-технічні заходи: ФПЗ та механізми захисту.	-	-	-	B_{54}	B_{55}	-	B_{57}
6	Додаткові програмно-технічні заходи: ФПЗ та механізми захисту.	B_{61}	B_{62}	B_{63}	B_{64}	B_{65}	B_{66}	B_{67}
7	Штатні організаційно-адміністративні заходи забезпечення гарантій безпеки середовища персоналу, стандартизації ТС, якості документації.	-	-	-	B_{74}	B_{75}	-	-
8	Додаткові організаційно-адміністративні заходи забезпечення гарантій безпеки.	B_{81}	B_{82}	B_{83}	B_{84}	B_{85}	B_{86}	B_{87}
9	Штатні організаційно-програмно-технічні заходи забезпечення гарантій спостережності і керованості ТС, конфіденційності і цілісності інформаційних ресурсів ТС.	-	-	-	B_{94}	B_{95}	-	B_{97}

ТС – технологічне середовище.

Для штатних програмно-технічних засобів враховуються етапи життєвого циклу: проектування, тестування, атестація, експлуатація. Супроводження штатних програмно-технічних заходів: ФПЗ та механізми захисту, входять до загальних витрат на технічну експлуатацію ЦКС. Деякі штатні ФПЗ та механізми захисту інформації залишились незадіяними в існуючій системі технічної експлуатації ЦКС але їх необхідно врахувати при обчисленні витрат на інформаційну безпеку.

Для додаткових засобів та механізмів захисту враховується повний життєвий цикл: пошук „слабких місць" та складання технічного завдання або технічних

умов, проектування, створення, оцінка або тестування, атестація, супроводження, експлуатація.

Загальні витрати на інформаційну безпеку можна визначити з виразу:

$$B_{\text{Á}} = \sum_{i=1}^{N}\sum_{j=1}^{M} B_{ij}, \qquad (5.8)$$

де M – кількість видів забезпечення інформаційної безпеки;

N – кількість статей витрат.

5.3.2 Приклад розрахунку на типовий вузол комутації

Використаємо методику розрахунку собівартості послуг міського телефонного зв'язку, сформовану на основі чинної нормативно-правової бази з урахуванням системи управлінського обліку вітчизняних операторів телекомунікацій.

Критерієм для розподілення усіх статей витрат пропонується взяти частку $ФЗП_{АТС}$ (фонд заробітної плати працівників штату цифрової АТС):

$$d_{\text{фзп АТС}} = ФЗП_{АТС} / ФЗП. \qquad (5.9)$$

Річний фонд заробітної плати за кожною j-ою ділянкою робіт визначається:

$$ФЗП_{АТСj} = З * Ш_j * (1 + Н_{фзп}) 12, \qquad (5.10)$$

де З – середньомісячна заробітна плата працівника цифрової АТС;

$Ш_j$ – штат за j-ою ділянкою робіт;

$Н_{фзп}$ – норматив відрахувань на соціальні заходи.

Частка фонду заробітної плати для кожної j-ої ділянки робіт розраховується за формулою:

$$d_{\text{фзп АТС}j} = ФЗП_{АТС\,j} / ФЗП_{АТС}\ . \qquad (5.11)$$

Амортизаційні відрахування за кожною j-ою ділянкою робіт обчислюються за формулою:

$$A_{АТСj} = d_{\text{фзп АТС}} * A_{АТС,} \qquad (5.12)$$

де $A_{АТС}$ – амортизаційні відрахування по АТС.

Матеріальні витрати за кожною j-ою ділянкою робіт подаються у вигляді:

$$M_{АТСj} = d_{\text{фзп АТС}} * M_{АТС}, \qquad (5.13)$$

де $M_{АТСj}$ – матеріальні витрати по АТС.

Інші операційні витрати за кожною j-ою ділянкою робіт визначаються за формулою:

$$E_{АТСj} = d_{\text{фзп АТС}} * E_{АТСін}, \qquad (5.14)$$

де $E_{АТСін}$ – інші витрати по АТС.

Далі розподіляються витрати ділянок (ФПЗ) відповідно до нормативного документа НД ТЗІ 2.5-002-99.

Середнє число працівників, зайнятих реалізацією функцій захисту, наведено з методики [8, 23] для 10-ої ділянки (ФПЗ) „Система захисту від збоїв та відмов у роботі АТС":

$$n_{\text{р}}=1-p_0 \qquad (3.15)$$

Для 10-ої ділянки n_p = 0,001356. При цьому p_0 = 0,998644.

Приклад розподілення витрат АТС за функціональними послугами захисту можна навести у вигляді табл. 5.3.

Таблиця 5.3 – Розподілення витрат АТС за функціональними послугами захисту

Статті витрат	*Номер j-ої ділянки роботи (ФПЗ)*												
	Виробничий штат												*Адміністративний штат*
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
1. Оплата праці з відрахуваннями ($ФЗП_{АТС\,j}$)	*Визначається відповідно до нормативного штату АТС та середньої заробітної плати*												
2. Амортизаційні відрахування ($A_{АТСj}$)	*Визначається відповідно до частки амортизаційних відрахувань у сумі витрат оператора або до частки амортизаційних відрахувань оператора у витратах на оплату праці оператора; за ділянками робіт розподіляється пропорційно до ФЗП для кожної з ділянок робіт*												
3. Матеріальні витрати ($M_{АТСj}$)	*Визначається відповідно до частки доходів від надання послуг АТС у сумі доходів оператора; або до частки матеріальних витрат оператора у витратах на оплату праці оператора; за ділянками робіт розподіляється пропорційно до ФЗП для кожної з ділянок робіт*												
4. Інші операційні витрати ($E_{АТСj}$)													
5. Усього витрат													
6. Структура витрат ($d_{ФЗП\,АТСj}$), %													

Вихідні дані :

А. Розмір витрат ФПЗ за статтями, грн.:

- оплата праці з відрахуваннями ФЗП – 138087600;
- амортизаційні відрахування А – 630000,00;
- матеріальні витрати М – 460000,00;
- інші операційні витрати Е – 355000,00.

Б. Штат оператора телекомунікацій, який залучено до надання ФПЗ, розраховано за нормативами чисельності штату, за ділянками робіт, осіб [22]:

1. Система захисту від впливів суб’єктів доступу через штатні термінали обслуговування і штатні прикінцеві пристрої – 0,45.

2. Система захисту від позаштатних впливів через штатні, або основні або штатні додаткові програми, і (або) технічні засоби – 0,3.

3. Системи захисту від позаштатних впливів на параметри середовища функціонування АТС – 0,3.

4. Система захисту від впливів позаштатними технічними і (або) програмно-технічними засобами на елементи устаткування в процесі експлуатації АТС – 0,7.

5. Система захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які установлені в процесі її експлуатації – 1,1.

6. Система захисту від впливів програмних закладок і (або) технічних закладних пристроїв, що установлені на передексплуатаційних стадіях життєвого циклу АТС – 0,3.

7. Система захисту від витоків інформації через канали ПЕМВН – 0,3.

8. Система захисту від витоків інформації через канали побічних акусто-електричних перетворень – 0,3.

9. Система захисту від якісної недостатності інформаційно вразливих режимів, функцій і послуг, що надаються АТС – 0,7.

10. Система захисту від збоїв та відмов у роботі АТС – 0,9986.

11. Система захисту від загроз у системах збереження інформації на фізичних носіях – 0,3.

12. Система ліквідації наслідків реалізованих загроз інформації – 1,1.

13. Система керування засобами ТЗІ – 1,0.

В. Середньомісячна заробітна плата – 839 грн.

Сукупністю всіх наведених ФПЗ створена множина засобів та механізмів захисту, які забезпечують ефективний та коректний захист.

При цьому під ефективністю засобу або механізму захисту розуміється його спроможність протистояти як прямим атакам, так і всіляким лазівкам, що пов’язані з роботою засобу або механізму захисту в конкретних умовах застосування (зокрема, спроможність протистояти відключенням, обходам, ушкодженням, обманам, провокуванням тощо).

Під коректністю засобу або механізму захисту розуміється його спроможність правильно реалізувати визначену ФПЗ.

Результати розрахунків витрат за ділянками робіт занесені у табл. 5.4, де наведено функціонально повний набір механізмів захисту інформації необхідних та достатніх для забезпечення заданого рівня захищеності АТС.

Витрати на штатні засоби і механізми інформаційної безпеки ЦКС на стадії її проектування і створення складають невелику частку загальних витрат. Вони включені у вартість систем, що постачаються, або у вартість будівництва об’єкта зв’язку.

Витрати на інформаційну безпеку на стадії технічної експлуатації ЦКС можуть досягати 20...25% загальних витрат на цій стадії. Значна їхня частина вже врахована в існуючій системі технічної експлуатації ЦКС.

Додаткові заходи і механізми забезпечення інформаційної безпеки, як правило, необхідні при досягненні високого рівня захищеності інформаційних ресурсів ЦКС. Для базового рівня захищеності частка витрат на додаткові засоби і механізми захисту може бути незначною.

Таблиця 5.4 – Розподілення витрат АТС за функціональними послугами захисту

Статті витрат	Номер *j*-ої ділянки роботи (ФПЗ)													
	Виробничий штат												Адмін. шт.	Усього
	1	2	3	4	5	6	7	8	9	10	11	12	13	
1. Оплата праці з відрахуваннями ($ФЗП_{АТСj}$), грн.	6243	4162	4162	9711	15261	4162	4162	4162	9711	13854	4162	15261	13873	
2. Амортизаційні відрахування ($А_{АТСj}$), грн.	2835	1890	1890	4410	6961	1890	1890	1890	4410	6300	1890	6961	6325	
3. Матеріальні витрати ($М_{АТСj}$), грн.	2070	1380	1380	3220	5083	1380	1380	1380	3220	4600	1380	5083	4618	
4. Інші операційні витрати ($Е_{АТСj}$), грн.	1597	1065	1065	2485	3922	1065	1065	1065	2485	3550	1065	3922	3564	
5. Усього витрат, грн.	112745	8497	8497	19826	31228	8497	8497	8497	19826	28304	8497	31228	28381	222523
6. Структура витрат ($d_{ФЗП\ АТСj}$), %	5,73	3,82	3,82	8,91	14,03	3,82	3,82	3,82	8,91	12,72	3,82	14,03	12.75	100

Найбільша частка витрат припадає на ділянки системи захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на АТС, які установлені в процесі її експлуатації (14,03%) та на систему ліквідації наслідків реалізованих загроз інформації на АТС (14,03%). Доцільність їх визначається при оцінках захищеності інформації та атестації КЗМЗ на відповідність вимогам системи ТЗІ.

5.4 Методика обґрунтування доцільності витрат на інформаційну безпеку ЦАТС

Методику обґрунтування доцільності та оцінку витрат на створення і впровадження системи забезпечення інформаційної безпеки будемо розглядати на прикладі цифрової АТС.

5.4.1 Якісний взаємозв'язок між витратами

Поділимо витрати на інформаційну безпеку за наступними категоріями на прикладі інформаційної безпеки цифрової АТС:

1. Витрати на формування та підтримку системи захисту інформації (витрати на організацію інформаційної безпеки).
2. Витрати на експлуатацію, тобто на технічне обслуговування системи захисту інформації та заходи із попередження порушень політики безпеки підприємства, на визначення та підтримку досягнутого рівня захищеності ресурсів цифрової АТС.
3. Запобігання збиткам – витрати, яких може зазнати організація в результаті того, що потрібного рівня захищеності не було досягнуто або при порушенні політики безпеки у випадках, пов'язаних з витоком інформації, втратою іміджу компанії, втратою довіри партнерів та споживачів тощо.
4. Загальні витрати, що включають витрати на організацію інформаційної безпеки, витрати на експлуатацію та запобігання збитків.

Класифікація витрат умовна, тому що збирання, класифікація та аналіз витрат на інформаційну безпеку – внутрішня справа підприємств, а детальне розроблення переліку залежать від особливостей конкретної організації. Головне при визначенні витрат на систему безпеки – взаєморозуміння та згода за статтями видатків усередині підприємства. Крім того, категорії витрат мають бути постійними та не дублювати один одного.

Неможливо повністю уникнути витрат на безпеку, однак вони можуть бути приведені до прийнятного рівня. Деякі види витрат на безпеку є абсолютно необхідними, а деякі можуть бути суттєво зменшені або виключені, наприклад, ті, які можуть зникнути при відсутності порушень політики безпеки або скоротяться, якщо кількість та руйнівний вплив порушень зменшаться.

При дотриманні політики безпеки та проведенні профілактики порушень можна виключити або суттєво зменшити наступні витрати:

– на відновлення ресурсів інформаційного середовища підприємства;
– на відновлення системи до відповідності вимогам політики безпеки;
– на відновлення ресурсів інформаційного середовища цифрової АТС;
– на переробку всередині системи безпеки;

– на юридичні суперечки та виплати компенсацій;

– на виявлення причин порушення політики безпеки.

Необхідні витрати – це ті, які необхідні навіть коли рівень загроз безпеці досить низький. Це витрати на підтримання досягнутого рівня захищеності інформаційного середовища цифрової АТС. Обов'язкові витрати можуть включати:

– обслуговування технічних засобів захисту;

– конфіденційне діловодство;

– функціонування та аудит системи безпеки;

– мінімальний рівень повірок та контролю з залученням спеціалізованих організацій;

– навчання персоналу методам інформаційної безпеки.

Сума всіх витрат на підвищення рівня захищеності підприємства від загроз інформаційної безпеки складає загальні витрати на безпеку, яка, однак, може бути зменшена за рахунок економії, що досягається за рахунок функціонування системи інформаційної безпеки. *Якісний взаємозв'язок між усіма витратами на безпеку, загальними витратами на безпеку та рівнем захищеності інформаційного середовища підприємства* зазвичай має вид функції (рис. 5.3).

Зі зміною рівня захищеності інформаційного середовища змінюються розміри складових загальних витрат та, відповідно, їхня сума – загальні витрати на безпеку.

На рис. 5.3 показано, що досягнутий рівень захищеності вимірюється за умовною якісною шкалою від 0 до 1,

де 0 – повна відсутність захищеності;

1 – абсолютна захищеність, яка на практиці ніколи не може бути досягнута.

Розглядаючи ліву сторону графіка, ми бачимо, що загальні витрати на інформаційну безпеку високі здебільшого тому, що високі витрати на компенсацію (запобігання збиткам) при порушеннях політики безпеки цифрової АТС. Витрати на обслуговування системи безпеки дуже малі.

Припустимо, що частка витрат на інформаційну безпеку збільшується. Це відповідає руху вправо рис. 5.3 за графіком.

Якщо ми будемо рухатися вправо за графіком, то досягнутий рівень захищеності буде збільшуватися, а інформаційний ризик знижуватися. Це відбувається за рахунок збільшення коштів на організацію безпеки.

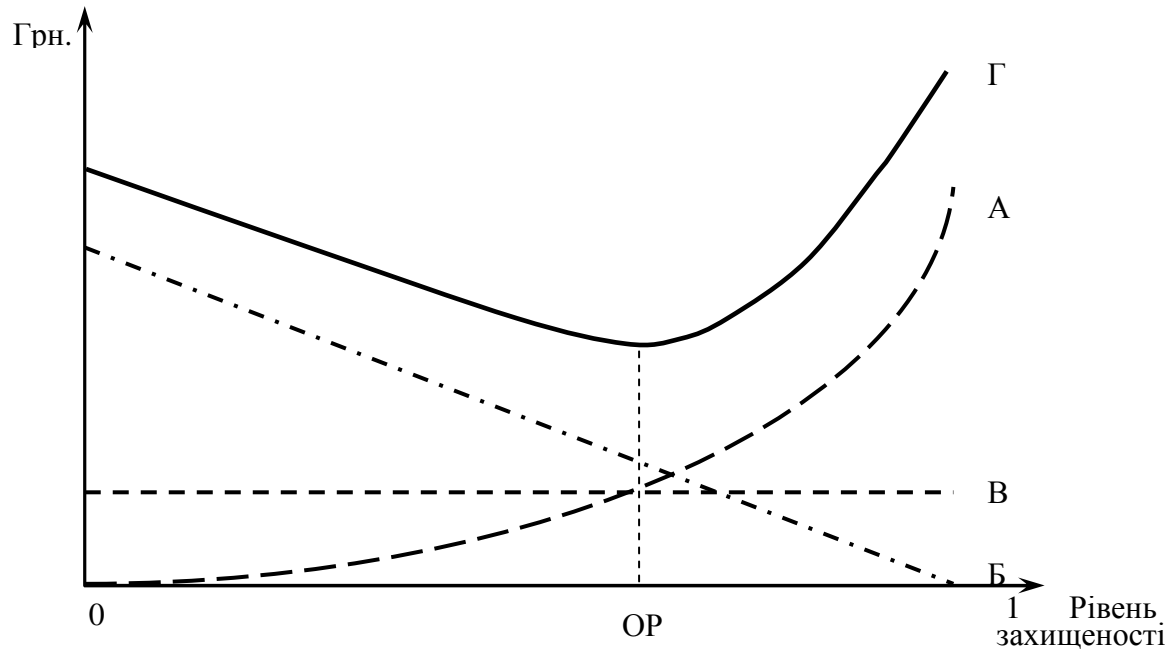

Рисунок 5.3 – Взаємозв'язок між витратами на інформаційну безпеку та досягнутим рівнем захищеності

Позначення: А – витрати на організацію інформаційної безпеки; Б – запобігання збиткам; В – витрати на експлуатацію системи інформаційної безпеки; Г – загальні витрати (крива, що характеризує ефективність системи інформаційної безпеки, яка включає витрати на організацію та експлуатацію, а також економію коштів, якої досягають при створенні системи інформаційної безпеки); ОР – оптимальний рівень захищеності та витрат на інформаційну безпеку (точка економічної рівноваги)

Запобігання збиткам зменшується в результаті попереджувальних заходів. Як показано на графіку, на цьому етапі витрати на компенсацію запобігання збитків падають швидше, ніж зростають витрати на організацію інформаційної безпеки цифрової АТС. Як результат – загальні витрати на безпеку зменшуються. Зміна об'єму витрат на експлуатацію незначна.

Якщо рухатись за графіком вправо за точку економічної рівноваги (тобто, коли рівень захищеності росте), то ситуація починає змінюватись. Добиваючись стійкого зниження витрат на запобігання збиткам від порушення політики безпеки, ми бачимо, що витрати на організацію певного рівня інформаційної безпеки зростають все швидше і швидше. Виходить, що значна кількість коштів може бути витрачена на досягнення досить малого зниження рівня ризику.

Рис. 5.3 відображає лише загальний випадок, оскільки його побудовано з урахуванням певних припущень, які не завжди відповідають реальним ситуаціям. Головне припущення полягає в тому, що точка економічної рівноваги не змінюється в часі. На практиці це припущення часто не виконується. Основні фактори:

– старіння системи інформаційної безпеки;

– розробники засобів захисту не встигають за активністю зловмисників, які знаходять все нові й нові слабкі місця в системах захисту.

Крім того, інформатизація підприємства може викликати нові проблеми, вирішення яких потребує додаткових витрат на організацію інформаційної безпеки. Все це може змістити економічну рівновагу у напряму до лівого краю графіка.

З проведеного дослідження випливає, що у структурі витрат на інформаційну безпеку головну позицію займають витрати на організацію інформаційної безпеки, оскільки їх збільшення веде до зменшення витрат на компенсацію (запобігання збиткам), а витрати на експлуатацію системи безпеки практично не змінюються.

5.4.2 Методичні основи обґрунтування витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі ЦАТС

Сфера використання методичних основ.

1. Методичні основи обґрунтування доцільності витрат на запровадження системи інформаційної безпеки програмно-керованих АТС призначена для визначення ефективності витрат на стадіях їх життєвого циклу – проектування системи інформаційної безпеки, створення, випробування та впровадження.

2. Методичні основи містять короткий опис методу розрахунків, порядок розрахунків ефективності витрат на інформаційну безпеку АТС, приклади розрахунків та коментарі до основних положень.

3. Методичні основи призначені для працівників підрозділів ТЗІ та економістів.

4. Результати визначення ефективності витрат мають використовуватися для вирішення таких завдань:

– вибору варіантів побудови системи інформаційної безпеки АТС та прогнозів ефективності від їхнього здійснення;

– планування та раціональний розподіл ресурсів за етапами життєвого циклу системи інформаційної безпеки АТС;

– визначення фактичної економічної ефективності системи інформаційної безпеки АТС, зокрема її впливу на економіку підприємства.

5. На основі обґрунтування формується техніко-економічне завдання виконавцям на проектування і створення системи інформаційної безпеки АТС. Ключовими його показниками є величина, яка відбиває ефективність застосування, що забезпечена за певний період, та величина відвернутих збитків внаслідок можливої реалізації загроз інформаційній безпеці.

Основні положення.

1. Визнаними в практиці основними показниками, що акумулюють вигоди упровадження системи інформаційної безпеки, є:

– чистий дисконтований доход, який у даному випадку представлено відвернутими втратами від реалізації загроз інформаційній безпеці;

– період окупності інвестицій у реалізацію системи інформаційної безпеки;

– внутрішня норма прибутковості.

Пояснення щодо економічної суті економічних показників та методи їх визначення наведені у прикладі розрахунків цього підрозділу.

2. Кількісна методика обґрунтування витрат на інформаційну безпеку є методом розрахунку техніко-економічної ефективності впровадження системи інформаційної безпеки в АТС, в якому фінансова вигода забезпечується щорічними збереженнями, які отримані при впровадженні системи інформаційної безпеки

$$A_{\text{щек}}=A_{\text{втр}}\,E - A_{\text{вит}}\,, \qquad (5.16)$$

де $A_{\text{щек}}$ – величина щорічної економії;

$A_{\text{втр}}$ – показник очікуваних втрат;

E – коефіцієнт ефективності системи захисту (його можна назвати коефіцієнтом психологічної ефективності системи захисту), E = 0,85.

$A_{\text{вит}}$ – щорічні витрати на інформаційну безпеку.

3. Визначення показника очікуваних втрат $A_{\text{втр}}$ засноване на знанні Власником цінності своєї інформації та емпіричних відомостях про вторгнення, про втрати від вірусів, про відбиття атак на ресурси тощо. Порушення безпеки може приводити до фінансових втрат, зв'язаних з:

– простоями та виходом з ладу станційного та мережного обладнання;

– нанесенням шкоди іміджу та репутації підприємства;

– оплатою робіт із відновлення роботи системи, програмного забезпечення тощо;

– витратами по судочинству тощо.

4. Початкові дані для оцінки можуть бути одержані трьома способами:

– збиранням статистичних даних за попередній період про загрози, їхню номенклатуру й частоту, втрати, понесені від загроз – фінансові, моральні, матеріальні, а також використанням результатів обстеження АТС як об'єкта інформаційної діяльності;

– використанням статистичних даних аналогічних українських підприємств, які діють у тому ж правовому полі;

– використанням статистичних даних зарубіжних фірм з урахуванням особливостей українського законодавства, умов підприємницької діяльності та нормативно-правових документів сфери ТЗІ. У прикладі розрахунку використано останній спосіб.

5. Для одержання оцінки очікуваних втрат використовують таблицю оцінки загроз та ризиків, яка дає можливість кількісно оцінити ймовірності подій. В таблиці взаємозв'язуються ймовірності загроз, міра небезпечності загроз і частота подій. Загальні очікувані втрати обчислюються як сума очікуваних втрат з кожної потенційної загрози. Приклад заповнення такої таблиці наведено у табл. 5.5. Користуючись результатами обстеження об'єкта інформаційної діяльності та матеріалами розробленої моделі загроз складається перелік загроз інформаційної безпеки і заповнюється стовпчик 2 таблиці розрахунку показника очікуваних втрат. Таблиця заповнюється у такому порядку:

- річна частота виникнення визначається відповідно до статистичних матеріалів ймовірності загроз і записується у стовпчик 3.

- втрати розраховуються на основі статистичних даних, які зібрані на даному або на інших аналогічних підприємствах, і записуються у стовпчик 4.

- внесок кожної потенційної загрози обчислюється у відсотковому відношенні і записується у стовпчик 5.

$A_{втр}$ розраховується за формулою (5.17) і записуються у стовпчик 6.

У даному випадку маємо відповідно:

$A_{втр1} = 0,6 * 348,4 = 209,04$ грн.;
$A_{втр2} = 1,0 * 402 = 402$ грн.;
$A_{втр3} = 36 * 495,8 = 17848,4$ грн.;
$A_{втр4} = 36 * 790,6 = 28461,6$ грн.;
$A_{втр5} = 12,0 * 1425,76 = 17109,12$ грн.;
$A_{втр6} = 12,0 * 951,4 = 111416,8$ грн.;
$A_{втр7} = 0,6 * 1407 = 844,2$ грн.;
$A_{втр8} = 1,0 * 1988,56 = 1988,56$ грн.;
$A_{втр9} = 1,0 * 2546 = 2546$ грн.;
$A_{втр10} = 1,0 * 6003,2 = 6003,2$ грн.;
$A_{втр11} = 36,0 * 10441,28 = 375886,08$ грн.

Підсумовуючи дані колонки 6 табл. 5.5 отримуємо показник очікуваних втрат $A_{втрΣ} = 462715$ грн.

Таблиця 5.5 – Розрахунок показника очікуваних втрат

№ пп.	Потенційні загрози	Частота виникнення, f	Втрати, грн., L	Втрати, %	$A_{втр,}$ грн.
1	Саботаж	0,6	348,4	1,3	209,04
2	Проникнення у систему	1,0	402	1,5	402
3	Атаки на ПЕОМ управління	36	495,8	1,85	17 848,4
4	Помилки в роботі з базою даних	36	790,6	2,95	28 461,6
5	Телефонне шахрайство	12,0	1425,76	5,32	17 109,12
6	Неавторизований доступ	12,0	951,4	3,55	11 416,8
7	Крадіжка обладнання і програм	0,6	1407	5,250	844,2
8	Фінансове шахрайство	1,0	1988,56	7,42	1 988,56
9	Помилки в роботі мережі сигналізації, синхронізації та керування	1,0	2546	9,5	2 546
10	Крадіжка приватної інформації	1,0	6003,2	22,4	6 003,2
11	Віруси	36,0	10441,28	38,96	375 886,08
12	Всього		26800	100,00	462 715

6. Показник $A_{втр}$ обчислюється за формулою:

$$A_{втр} = f * L, \qquad (5.17)$$

де f – частота виникнення потенційної загрози, рівень якої визначається на основі ймовірності загроз;

L – величина втрат у гривнях, яка визначається на основі небезпечності порушення.

Для тих загроз, на які відсутні статистичні дані про частоту їхнього виникнення, використовують якісні шкали. Частоту виникнення таких загроз визначають використовуючи залежність між частотою й якісною оцінкою ймовірності. Приклад такої залежності показано у табл. 5.6.

7. Витрати на створення системи інформаційної безпеки поділяють на одноразові і періодичні. Одноразові витрати складаються з витрат на купівлю апаратних засобів, програмного забезпечення, проектування системи.

Періодичні витрати складаються з витрат на технічне обслуговування та супроводження, заробітну плату персоналу, навчання та підвищення кваліфікації спеціалістів, витрат на дослідження загроз порушення політики безпеки.

Таблиця 5.6 – Приклад середньорічної ймовірності загроз

Рівень ймовірності	Опис	Частота
1	2	3
Незначний	Навряд відбудеться	0,05
Дуже низький	Подія відбувається два-три рази на 5 років	0,6
Низький	Подія відбувається менше одного разу на рік або раз на рік	1,0
Середній	Подія відбувається менше одного разу на півріччя або раз на півріччя	2,0
Високий	Подія відбувається менш одного разу на місяць або раз на місяць	12,0
Дуже високий	Подія відбувається декілька разів на місяць	36,0
Екстремальний	Подія відбувається декілька разів на день	365,0

8. Далі витрати на впровадження системи захисту, розрахунок періоду окупності та економічної ефективності, приведені вартості розраховують класичним методом. Порядок розрахунку наведено нижче.

Порядок розрахунків:

1. Після визначення показника очікуваних втрат приймається рішення про створення системи інформаційної безпеки і проводиться розрахунок її економічної ефективності.

2. Обираються вхідні дані за статтями витрат на купівлю ліцензії, на проектні роботи, на технічну підтримку. Норматив витрат на технічну підтримку складає 30% від вартості ліцензії. Витрати на впровадження системи захисту інформації розраховуються за наступною формулою:

$$C_{\text{впр}} = C_{\text{л}} + C_{\text{пр}} + \sum_{s} C_i, \qquad (5.18)$$

де $C_{впр}$ – витрати на впровадження;

$C_л$ – витрати на купівлю ліцензії;

$C_{пр}$ – витрати на проектні роботи;

C_i – витрати на технічну підтримку.

Період окупності інвестиційних проектів, пов'язаних з впровадженням інформаційних технологій, не повинен бути більшим ніж три роки, тому період оцінки ефективності даного проекту впровадження дорівнює трьом рокам.

Витрати на проектні роботи розподіляються на першому році. Витрати на технічну підтримку розподіляються на подальший період впровадження.

Результати цього і наступних розрахунків зручно і наглядно зводити в таблицю розрахунку показника повернення інвестицій на систему інформаційної безпеки.

Приклад такої таблиці та розрахунків оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової АТС наводиться у табл. 5.8 у розділі 5.4.3.

3. Розраховуються на кожен рік накопичені витрати проекту впровадження за формулою:

$$\begin{aligned} C_{нак\ 1} &= C_{нак\ поч.} + C_{впр1,} \\ C_{нак\ 2} &= C_{нак\ 1} + C_{впр2,} \\ C_{нак\ 3} &= C_{нак\ 2} + C_{впр3,} \end{aligned} \qquad (5.19)$$

де $C_{нак}$ – накопичені витрати проекту впровадження;

$C_{впр}$ – витрати на впровадження.

4. Розраховується на кожен рік накопичений чистий грошовий потік витрат на впровадження за формулою:

$$NPV_в = \sum_{i=0}^{2} \frac{CF}{(1+r)^i}, \qquad (5.20)$$

де $NPV_в$ – накопичений чистий грошовий потік витрат на проект впровадження;

CF – грошовий потік витрат на впровадження;

r – ставка дисконтування.

Роль грошового потоку відіграють витрати на впровадження. Ставка дисконтування дорівнює ставці рефінансування Національного Банку України, $r = 15\%$.

5. Обираються з фінансових та технічних звітів підприємства, показники загальної вартості володіння *(TCO – Total Cost of Ownership)*:

$TCO_п$ – поточний показник *TCO*;

$TCO_ц$ – цільовий показник *TCO*;

$TCO_ф$ – фактичний показник *TCO*.

6. Розраховуються вигоди при оптимізації показника загальної вартості володіння за формулою:

$$В = TCO_n - TCO_ф, \qquad (5.21)$$

де В – накопичений показник вигод при оптимізації показника *TCO*;

$TCO_{\text{п}}$ – поточний показник *TCO*;

$TCO_{\text{ф}}$ – фактичний показник *TCO*.

7. Розраховуються величини щорічної економії за формулою:

$$A_{\text{щек}} = A_{\text{втр}} * E - A_{\text{вит}}, \tag{5.22}$$

де $A_{\text{щек}}$ – величина щорічної економії;

$A_{\text{втр}}$ – показник очікуваних втрат;

E – коефіцієнт ефективності системи захисту (коефіцієнт психологічної ефективності системи захисту);

$A_{\text{вит}}$ – щорічні витрати на інформаційну безпеку, $A_{\text{вит}} = TCO_{\text{ф}}$

8. Розраховується показник вигод при оптимізації показника *TCO* та щорічної економії за формулою:

$$\text{В}_{tco} = \text{В} + A_{щек}, \tag{5.23}$$

де В_{tco} – показник вигод при оптимізації показника *TCO* та щорічних збережень;

В – вигоди при оптимізації показника *TCO*;

$A_{\text{щек}}$ – величина щорічної економії.

9. Розраховується накопичений показник вигод при оптимізації показника *TCO* та щорічної економії за формулою:

$$\begin{aligned} \text{В}_{\text{нак 1}} &= \text{В}_{tco1}, \\ \text{В}_{\text{нак 2}} &= \text{В}_{\text{нак 1}} + \text{В}_{tco2}, \\ \text{В}_{\text{нак 3}} &= \text{В}_{\text{нак 2}} + \text{В}_{tco3} \end{aligned} \tag{5.24}$$

де $\text{В}_{\text{нак}}$ – накопичений показник вигод при оптимізації показника *TCO* та щорічної економії;

В_{tco} – показник вигод при оптимізації показника *TCO* та щорічних збережень.

10. Розраховується грошовий потік за формулою:

$$CF = \text{В}_{tco} - C_{\text{впр}}, \tag{5.25}$$

де *CF* – грошовий потік;

В_{tco} – показник вигод при оптимізації показника *TCO* та щорічних збережень;

$\text{С}_{\text{впр}}$ – витрати на впровадження.

11. Розраховується накопичений грошовий потік за формулою:

$$CF_{\text{нак}} = \text{В}_{\text{нак}} - C_{\text{нак}}, \tag{5.26}$$

де $CF_{\text{нак}}$ – накопичений грошовий потік;

$\text{В}_{\text{нак}}$ – накопичений показник вигод при оптимізації показника *TCO* та щорічної економії;

$C_{\text{нак}}$ – накопичені витрати проекту впровадження.

12. Розраховується накопичений чистий грошовий потік доходів (відвернутих витрат) від проекту впровадження за наступною формулою:

$$NPV_{\text{д}} = \sum_{i=0}^{2} \frac{CF}{(1+r)^i}, \qquad (5.27)$$

де $NPV_{\text{д}}$ – накопичений чистий грошовий потік відвернутих доходів від проекту впровадження;

CF – грошовий потік (вигоди від оптимізації показника ТСО та впровадження корпоративної системи захисту);

r – ставка дисконтування.

Ставка дисконтування у цій формулі приймається за r = 25%. Це дасть можливість обчислити далі внутрішню норму прибутковості.

13. Розраховується внутрішня норма прибутковості (*IRR*). Розрахунок проводиться графічним способом. На графіку будується пряма, яка з'єднує точку накопиченого чистого грошового потоку на проект $NPV_{\text{в}}$ при ставці дисконтування r = 15% з точкою, яка відповідає накопиченому чистому грошовому потоку відвернутих витрат від проекту впровадження – $NPV_{\text{д.}}$ при ставці дисконтування r = 25%.

Точка, де пряма перетинає вісь абсцис є внутрішньою нормою прибутковості. Прибутковість тут має значення відвернутих збитків, які могли б бути за відсутності системи інформаційної безпеки.

5.4.3 Приклад розрахунку оцінки витрат на інформаційну безпеку ЦАТС

Обираємо вхідні дані за статтями витрат, які наводимо в табл. 5.7.

Таблиця 5.7 – Вихідні дані для розрахунку

№ пп.	Статті витрат	Вартість, грн.
1	Витрати на купівлю ліцензії	150 000
2	Витрати на проектні роботи	3 500
3	Технічна підтримка (30% від вартості ліцензії щорічно)	45 000

Розраховуємо $C_{\text{впр}}$ – витрати на впровадження системи захисту інформації за формулою (3.18) та розподіляємо їх на три роки. Витрати на проектні роботи розподіляємо на першому році.

Витрати на технічну підтримку розподіляємо на подальший період впровадження. Ці і подальші результати обчислень зводимо в таблицю розрахунку оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки (табл. 5.8).

Розраховуємо на кожен рік $C_{\text{нак}}$ – накопичені витрати проекту впровадження за формулами (3.19). Маємо послідовно:

$C_{\text{нак 1}}$ =150 000 + 3500 = 153 500 грн.;

$C_{\text{нак 2}}$ = 153 500+45 000 = 198 500 грн.;

$C_{\text{нак 3}}$ = 198 500 + 45000 = 243 500 грн.

Результати заносимо в табл. 5.8

Розраховуємо *NPV* – накопичений чистий грошовий потік витрат на впровадження за формулою (3.20).

За три роки маємо *NPV* = 150 000 * 0,15 = 22500 грн. Цей результат заносимо у другий стовпчик табл. 5.8.

Робимо на кожен рік вибірку з фінансових та технічних звітів підприємства показників загальної вартості володіння *(ТСО)*:

$ТСО_{п}$ – поточного показника ТСО;

$ТСО_{ц}$ – цільового показника ТСО;

$ТСО_{ф}$ – фактичного показника ТСО.

Результати вибірки заносимо в табл. 5.8.

Розраховуємо на кожен рік та в цілому за три роки *В* – накопичений показник вигоди при оптимізації показника загальної вартості володіння та щорічні збереження за формулою (3.21).

Таблиця 5.8 – Розрахунок оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової АТС

№ п.п	Показники	Початкові витрати, грн.	Роки			
			1	2	3	Всього, грн.
1	Витрати на впровадження, $С_{впр}$	150 000	3 500	45 000	45 000	243 500
2	Накопичені витрати проекту впровадження, $С_{нак}$	150 000	153 500	198 500	243 500	-
3	Накопичений чистий грошовий потік *(NPV)* витрат на проект впровадження, $NPV_{в}$	22 500	-	-	-	-
4	Поточний показник *ТСО,* $ТСО_{п}$	-	8 794,58	8 794,58	8 794,58	26 383,74
5	Цільовий показник *ТСО,* $ТСО_{ц}$	-	6 621,64	6 621,64	6 621,64	19 864,92
6	Фактичний показник *ТСО,* $ТСО_{ф}$	-	8 359,99	7 273,52	6 621,64	22255,15
7	Вигоди при оптимізації показника *ТСО,* В	0	434,59	1521,06	2172,94	4128,59
8	Показник очікуваних втрат $А_{втр}$	0	462 715	462 715	462 715	1 388 145
9	Ефективність системи корпоративного захисту, *Е*	-	85%	85%	85%	-
10	Величина щорічної економії, $А_{щек}$	0	384 947,7	386 034,23	386 686,11	1 157 668,1
11	Показник вигод при оптимізації показника *ТСО* та щорічної економії, $В_{тсо}$	0	385 382, 3	387 555,29	388 859,05	1 161 796,7
12	Накопичений показник вигод при оптимізації показника *ТСО* та щорічної економії, $В_{нак}$	0	385 382, 3	772 937,64	1 161 796,7	-
13	Грошовий потік, *CF*	- 150 000	381 882,3	342 555,29	343 859,05	918 296,69
14	Накопичений грошовий потік, $CF_{нак}$	- 150 000	231 882,3	574 437,63	918 296,69	-

15	Накопичений чистий грошовий потік *(NPV)* доходів впровадження $NPV_д$	- 37 500	-	-	-	-
16	Внутрішня норма прибутковості, *IRR*	18,5%	-	-	-	-

Маємо послідовно:

$В_1$ = 8794,58 – 8359,99 = 434, 59 грн.;

$В_2$ = 8794,58 – 7273,52 = 1521,06 грн.;

$В_3$ = 8794,58 – 6621,64 = 2172,94 грн.;

$В_Σ$ = 434,59 + 1521,06 + 2172,94 = 4128,59 грн.

Результати обчислень заносимо в табл. 5.8.

Записуємо у табл. 5.8 величину показника очікуваних втрат $A_{втр}$ та величину коефіцієнта ефективності системи корпоративного захисту (коефіцієнт психологічної ефективності) *E,* $A_{вит i} = TCO_{фі}$. Розраховуємо $A_{щек}$ – величини щорічних збережень за формулою (3.22).

Маємо послідовно:

$A_{щек\ 1} = A_{втр} * E - A_{вит\ 1}$ = 462 715 * 0,85 – 8359,99 = 384 947,76 грн.;

$A_{щек\ 2} = A_{втр} * E - A_{вит\ 2}$ = 462 715 * 0,85 – 7273,52 = 386 034,23 грн.;

$A_{щек\ 3} = A_{втр} * E - A_{вит\ 3}$ = 462 715 * 0,85 – 6621,64 = 386 686,11 грн;

$A_{щекΣ} = A_{втр} * E - A_{вит\ Σ}$ =1 388 145 * 0,85 – 22255,15 = 1 157 668,1 грн.

Результати обчислень заносимо в табл. 5.8

Розраховуємо на кожен рік та в цілому показник вигод при оптимізації показника *TCO* та щорічних збережень $В_{тco}$ за формулою (3.23).

Маємо послідовно:

$В_{тco1} = В_1 + A_{щек1}$ = 434,59 + 384 947,76 = 385 382,35 грн.;

$В_{тco2} = В_2 + A_{щек2}$ = 1521,06 + 386034,23 = 387 555,29 грн.;

$В_{тco3} = В_3 + A_{щек3}$ = 2172,94 + 386 686,11 = 388 859,05 грн.;

$В_{тcoΣ} = В_{тco1} + В_{тco2} + В_{тco3}$ = 385 382,35 + 387 555,29 + 388 859,05 = = 1 161 796,69 грн.

Результати обчислень заносимо в табл. 5.8.

Розраховуємо на кожен рік накопичений показник вигод при оптимізації показника *TCO* та щорічні збереження за формулами (3.24).

Маємо послідовно:

$В_{нак\ 1}$ = 385 382,35 грн.;

$В_{нак\ 2}$ = 385 382,35 + 387 555,29 = 772937,64 грн.;

$В_{нак\ 3}$ = 772937,64 + 388 859,05 = 1 161 796,69 грн.

Результати обчислень заносимо в табл. 5.8.

Розраховуємо на кожен рік та в цілому грошовий потік *CF* за формулою (3.25). Маємо послідовно:

$CF_1 = B_{тco1} - C_{впр1}$ = 385 382,35 – 3500 = 381 882,35 грн.,

$CF_2 = B_{тco2} - C_{впр2}$ = 387 555,29 – 45 000 = 342 555,29 грн.,

$CF_3 = B_{тco3} - C_{впр3}$ = 388 859,05 – 45 000 = 343 859,05 грн.,

$CF_Σ = CF_1 + CF_2 + CF_3$ = 385 382,35 + 342 555,29 + 343 859,05 = = 918 296,69 грн. Результати обчислень заносимо в табл. 5.8.

Розраховуємо на кожен рік накопичений грошовий потік $CF_{нак}$ за формулою (3.26). Маємо послідовно:

$CF_{нак1}$ = $В_{нак1}$ – $С_{нак1}$ = 385 382,35 – 153 500 = 231 882,35 грн.;

$CF_{нак2}$ = $В_{нак2}$ – $С_{нак2}$ = 772 937,63 – 198 500 = 574 437,63 грн.;

$CF_{нак3}$ = $В_{нак3}$ – $С_{нак3}$ = 1 161 796,69 – 243 500 = 918 296,69 грн.

Розраховуємо *NPV* – накопичений чистий грошовий потік витрат на проект впровадження та доходів від проекту впровадження за формулою (3.27). Ставка дисконтування у цій формулі приймається за r = 25%. Це дасть можливість обчислити далі внутрішню норму прибутковості.

Отриманий результат розрахунку *NPV* = – 150 000 * 0,25 = – 37 500 грн. заносимо в табл. 5.8.

Розраховуємо *IRR* – внутрішню норму прибутковості. Розрахунок проводиться графічним способом (рис. 5.4). На графіку будується пряма, яка з'єднує точку накопиченого чистого грошового потоку витрат на проект ($NPV_в$) при ставці дисконтування r = 15% з точкою, яка відповідає накопиченому чистому грошовому потоку доходів (відвернутих витрат) від проекту впровадження – $NPV_д$ при ставці дисконтування r = 25%.

Точка, де пряма перетинає вісь абсцис є внутрішньою нормою прибутковості. Прибутковість тут має значення відвернутих збитків, які могли б бути за відсутності системи інформаційної безпеки. З рис. 5.4 випливає, що *IRR* = 18,5%. При ставці дисконтування 18,5% поточна вартість очікуваних відвернутих збитків буде дорівнювати поточній вартості необхідних грошових вкладень.

Економічні аспекти впровадження системи інформаційної безпеки. Інноваційні інвестиції вкладення економічних ресурсів у систему інформаційної безпеки та їх впровадження з метою створення й одержання чистої вигоди на окремому господарському об'єкті господарювання.

Вигоди від використання системи інформаційної безпеки виявляються у вигляді відвернутих збитків, доходів підприємств, які надають послуги з захисту інформації, соціально-економічних та інших переваг.

Потік реальних грошей, за допомогою якого здійснюється оцінка вигоди від впровадження системи інформаційної безпеки, це відвернення платежів за збитками, або платежу (відтік реальних грошей як наслідок ефективного чи неефективного використання системи).

Якщо протягом певного періоду відвернуті збитки перевищують витрати, можна говорити про позитивні грошові потоки (*positive cash flows*).

Якщо витрати перевищують відвернуті збитки – мають місце чисті витрати (*net expenditure*) або відтоки грошових коштів (*cash outlay*). Уся серія грошових потоків, пов'язаних з інноваційним проектом, є потоком грошових коштів (*flow stream*).

Для виявлення вихідних даних, особливо потенційної можливої вигоди проекту, необхідна тісна взаємодія підприємств-замовників з розробниками технологій інформаційної безпеки та систематичне проведення моніторингу стану інформаційної безпеки з метою накопичення статистичних даних про загрози, атаки, величину збитків від атак та ефективності системи захисту.

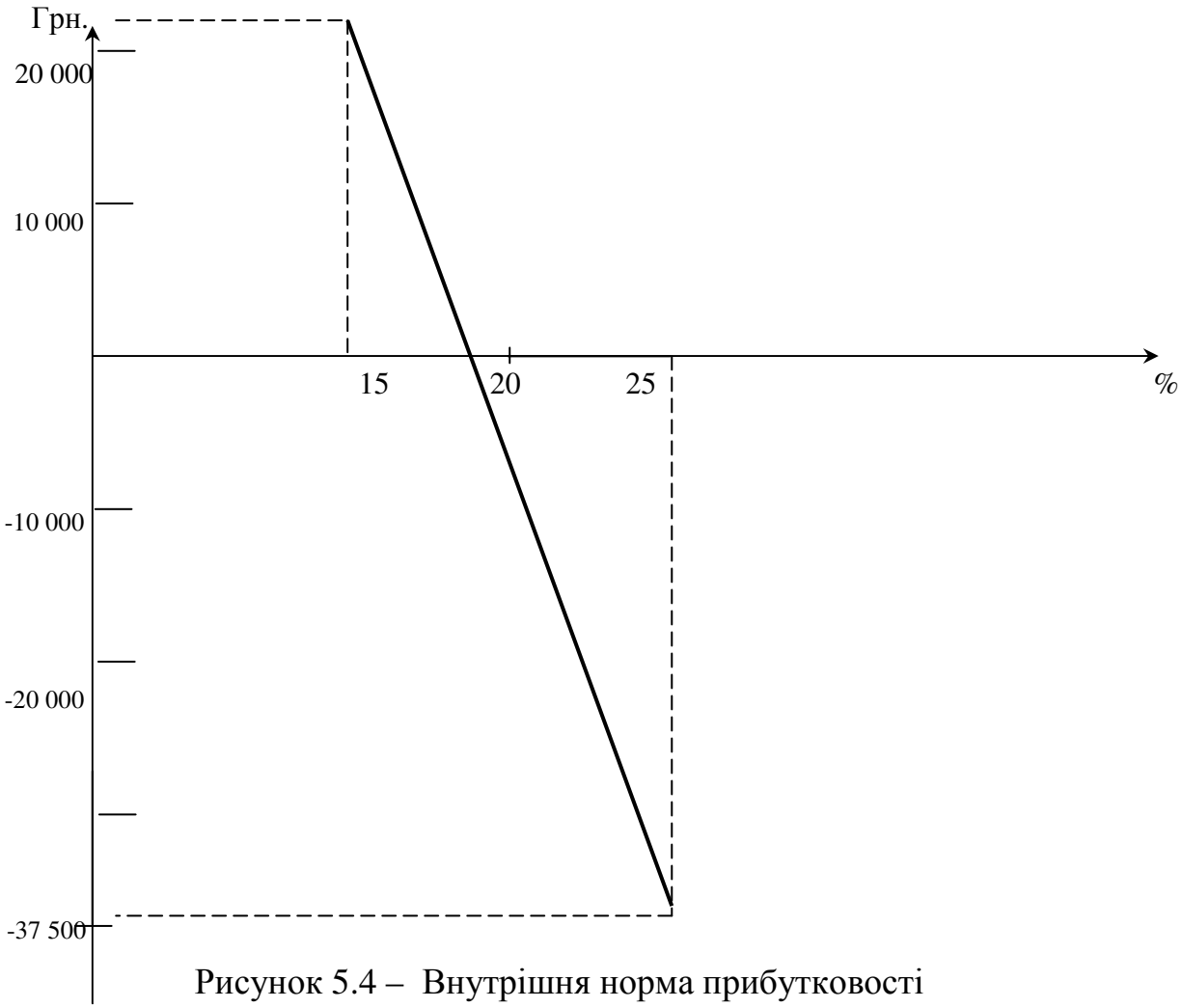

Рисунок 5.4 – Внутрішня норма прибутковості

Запитання для самоконтролю

1. На які категорії поділяються витрати на інформаційну безпеку?
2. Прокоментуйте структуру витрат на інформаційну безпеку ЦАТС.
3. Як оцінюється захищеність інформації від витоку її технічними чи фізичними каналами?
4. Поясніть особливості експертних методів оцінки параметрів інформаційної безпеки.
5. Дайте визначення понять „метод нечіткої логіки”, „нечітких множин” та „лінгвістичні змінні”. Яке вони мають застосування?
6. На які три класи можна поділити задачі аналізу показників захищеності інформаційних ресурсів?
7. Для чого використовують матрицю показників захищеності та якості телекомунікаційних мереж?
8. Поясніть методи відбору найбільш раціонального варіанта побудови системи інформаційної безпеки:
   8.1) диференційний метод;
   8.2) метод багатокритеріального оцінювання;
   8.3) метод комплексного показника;

8.4) інтерактивний метод.

9. Поясніть алгоритм вибору оптимального варіанта побудови системи інформаційної безпеки методом розв’язання задачі багатокритеріального вибору.

10. Яка структура витрат на інформаційну безпеку в типовій ЦАТС?

11. Як визначаються витрати за функціональними послугами захисту:

11.1) за оплатою праці;

11.2) за амортизаційними відрахуваннями;

11.3) за матеріальними витратами.

12. За якими чотирма категоріями поділяють витрати на інформаційну безпеку цифрової АТС?

13. Поясніть якісний взаємозв’язок між усіма витратами на безпеку, загальними витратами на безпеку та рівнем захищеності інформаційного середовища підприємства.

14. Який фізичний смисл «точки економічної рівноваги»?

15. Прокоментуйте методичні основи обґрунтування доцільності витрат на запровадження системи інформаційної безпеки програмно-керованих АТС.

16. Як знаходять частоту виникнення потенційних загроз?

17. Що необхідно для знаходження середньорічної ймовірності загроз?

18. Як розраховується внутрішня норма прибутковості (*IRR*)? Поясніть графік внутрішньої норми прибутковості.

6 КОМПЛЕКСНА СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦЕНТРУ ОБРОБКИ ВИКЛИКІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ

Законом України “Про телекомунікації” визначені ключові завдання забезпечення інформаційної безпеки телекомунікаційних мереж: охорона таємниці телефонних розмов, телеграфної, іншої кореспонденції; захист інформації з обмеженим доступом, що є власністю держави; захист державних інформаційних ресурсів; захист інформації про споживача; захист інформації, що передається телекомунікаційними мережами; забезпечення сталості, надійності та підтримки рівня якості та безпеки телекомунікаційних послуг.

Сильна інтеграція телекомунікаційних, мережних та комп’ютерних технологій приводить до об’єднання систем обробки, передачі та зберігання інформації. Практичним прикладом інтегрованої інформаційної технології є застосування універсальної інфокомунікаційної платформи для роботи з клієнтами: центрів обробки викликів (ЦОВ, *Call* - центрів) для побудови вузлу служб зв’язку телекомунікаційних мереж з розвинутими послугами для підприємств, організацій та населення [23]. Відкритість інформаційних систем, простота доступу до інформаційних ресурсів породжують багато проблем. У даному розділі викладаються:

- принципи побудови центрів обслуговування викликів для органів внутрішніх справ та інших органів державної влади, які побудовані на базі цифрових відомчих АТС та обладнання з комутацією пакетів (*IP* - контакт-центрів);
- методи розрахунку характеристик обслуговування, інформаційних потоків, обсягу обладнання та численності персоналу;
- вимоги до системи технічного захисту інформації об’єктів інформаційної діяльності органів внутрішніх справ;
- процедури проектування комплексної системи забезпечення інформаційної безпеки центрів обробки викриків.

6.1 Принципи автоматизації обробки викликів та надавання інформаційних та телекомунікаційних послуг

Центри обробки викликів – це універсальна система обміну повідомленнями, яка об’єднує комп’ютерну телефонію, комунікаційні мережі й використовує комп’ютерно-телефонну інтеграцію. Створення центрів стало можливим при розробці комплексу засобів комп’ютерно-телефонної інтеграції як сукупності рекомендацій та стандартів, спрямованих на взаємодію пристроїв телефонного зв’язку та комп’ютерної техніки. Окрім того, розроблено спеціальне програмне забезпечення для виконання функцій, раніше виконуваних оператором телефонного зв’язку. Усю основну роботу з обробки виклику виконує комплекс апаратного та програмного забезпечення. Використовуються алгоритми синтезу та розпізнавання мовлення й інтелектуальна система розподілу викликів.

ЦОВ призначено для різноманітних телефонних вузлів служб зв’язку: правоохоронних органів, швидкої допомоги, пожежної охорони, різних довідкових служб, систем для виконання замовлень та продажу квитків. Центри

можуть використовуватись для обслуговування абонентів, котрі користуються міжміським та міжнародним зв'язком, для вивільнення оператора від трудомістких монотонних операцій.

Залежно від характеру операції, котрі проводять ЦОВ, поділяються на: приймаючі дзвінки; такі, що займаються масовим обдзвонюванням; змішаного типу.

Функції центру обробки викликів. У ЦОВ здійснюється доступ до комп'ютерної бази даних, де зберігається інформація про абонентів. Частина даних, що заносяться в таку базу, вводяться оператором вручну, частину абонент може набирати сам за допомогою телефону, а частину визначає адміністрація телефонної мережі. Оператор має можливість короткого анкетування абонента при його першому дзвінкові до Центру.

Надаються інтелектуальні послуги такі, як телеголосування, використовується Інтернет. Водночас з переглядянням змісту *Web*-ресурсів може бути організовано передавання голосових повідомлень від клієнта до агентів і навпаки. Можлива організація розвинутої довідкової служби, служби контролю абонентських рахунків.

В Україні на телекомунікаційних мережах загального користування розпочато впровадження вузлів служб зв'язку з функціями *Call*-центру, які повинні забезпечувати обробку навантаження від звичайних послуг, високоякісних інтелектуальних послуг, а також навантаження з урахуванням доступу до мережі Інтернет. Економічна ефективність ЦОВ досягається за рахунок економії на організації внутрішніх потоків і підвищення якості обслуговування.

Є численні варіанти взаємодії агента (свого роду автоматичного оператора) й клієнта (споживача). ЦОВ забезпечує єдине середовище обміну повідомленнями поміж співробітниками підприємства та клієнтами (рис. 6.1). Усі повідомлення (факси, електронні листи тощо) обробляються в однаковий спосіб, що сприяє економії часу та персоналу. Тим самим знижуються витрати на обслуговування по телефону. Економія досягається за рахунок таких чинників: збільшення швидкості обробки викликів; раціональне використання високооплачуваних спеціалістів; скорочення чисельності операцій, що виконуються при обробці викликів, за рахунок реєстрації інформації, яка повідомляється абонентом; економія витрат на оплату телефонних розмов за безкоштовними номерами (послуга 800); автоматизація контролю за роботою оператора.

Функції ЦОВ реалізуються за допомогою спеціального програмного забезпечення. Головним є програмний комплекс автоматичного розподілу викликів. Усі операції реєструються і можуть бути подані у вигляді статистичної інформації щодо часових характеристик обслуговування клієнта, часу очікування тощо. У процесі обробки викликів діють оператори, що спеціалізуються на прикладних задачах.

Спеціальне програмне забезпечення (ПЗ) функціонує на виділеному сервері або групі серверів. Робочі місця агентів, як правило, обладнані комп'ютерними робочими станціями та/або спеціалізованими телефонними апаратами.

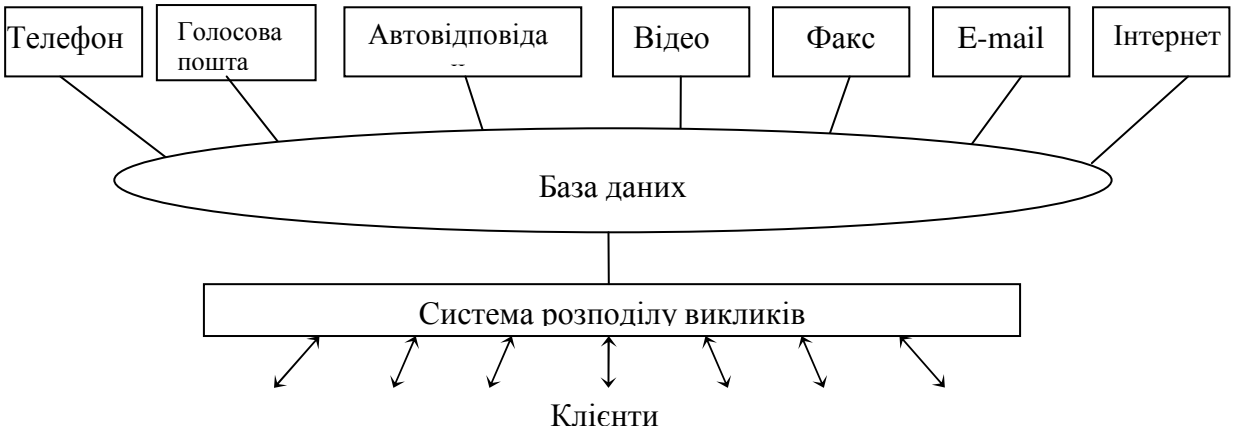

Рисунок 6.1 – Функціональна структура центру обробки

У стандарті R.100 Міжнародної організації *The Enterprise Computer Telephony Forum (ECTF)* оператор визначається так:

оператор (*агент*) – це людина або пристрій, основною функцією якого є обробка виклику.

Оператори ідентифікуються унікальним ім'ям або номером та мають кожен свій пароль, який запитується при реєстрації оператора на робочому місці, так званій консолі.

Комплекс може передавати виклики від одного оператора до іншого разом з усією інформацією залежно від інтенсивності та характеру виклику клієнтів. Це оптимізує завантаження операторів та скорочує час обробки.

Структура та принципи функціонування центрів обробки викликів. Варіант архітектури ЦОВ подано на рис. 6.2.

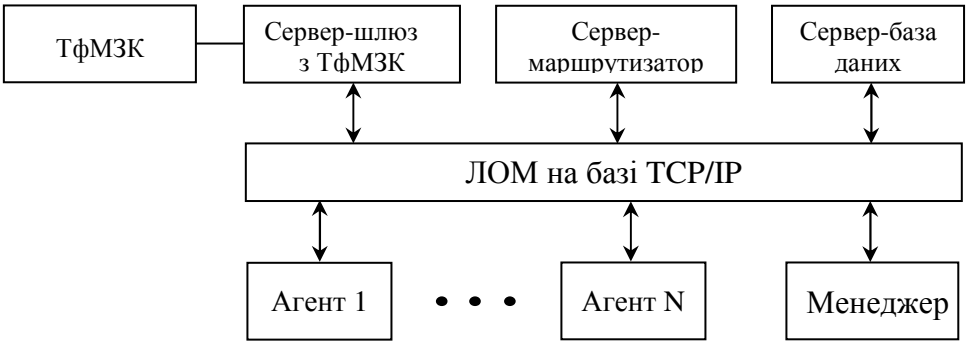

Рисунок 6.2 – Функціональна структура центру обробки викликів

Перші варіанти побудови телефонно-комп'ютерного ЦОВ реалізовувались із застосуванням установчо-виробничої комутаційної станції та телекомуніка-ційного сервера.

Більш гнучкі ЦОВ можуть базуватись на застосуванні стандартів *Voise over IP* (наприклад H.323, котрий регламентує протоколи передавання телефонії *IP*-мережею).

Продуктивність центру залежить від пропускної здатності його складових частин: шлюзу для сполучення з телефонною мережею загального користування (ТфМЗК); внутрішньої *IP* - мережі (локальної обчислювальної

мережі – ЛОМ); маршрутизатора для реалізації логіки маршрутизації *IP* - пакетів; бази даних. Для реалізації шлюзу виробляються спеціалізовані плати шлюзу "голос – *IP* - мережа", котрі дозволяють приєднати гарнітуру оператора й набирати номер на клавіатурі. Виклик приймається комп'ютером, і всі дії оператор виконує через комп'ютер. Цифровий сигнальний процесор такої плати реалізує алгоритм стискання мовлення за протоколом G.721 або G.729 із затримкою голосового сигналу не більше за 55 мс. Комп'ютери підключаються через інтерфейс *RS*-232 або адаптер *Ethernet*.

Відомча АТС (ВАТС) підключається до ТфМЗК багатоканальною з'єднувальною лінією. Ємність та тип такого з'єднання визначаються потоками запитів, якими оперує ЦОВ, та максимальною кількістю агентів, що працюють в одну зміну. З'єднувальний тракт може бути зорганізовано каналами Е1 або волоконно-оптичною лінією зв'язку. Як правило, ВАТС доповнюється комунікаційним пристроєм (окремим блоком) для сполучення з комп'ютерною мережею. Його функція – забезпечити обмін повідомленнями поміж ВАТС та комп'ютерною системою. Функціонування ЦОВ покажемо за допомогою схеми функціональної взаємодії апаратно-програмного забезпечення (рис. 6.3).

Основними взаємодіючими програмно-апаратними функціональними одиницями ЦОВ є комунікаційний сервер, база даних, система автоматичного дозвонювання, система інтерактивного голосового обміну, сервер баз даних та сервер статистики.

Комунікаційний сервер забезпечує можливість обробки викликів і є безпосередньо сполучений з комунікаційним пристроєм. Він є центральним вузлом збирання та розподілу будь-якої інформації телефонних з'єднань. Головна особливість полягає в інтеграції всіх функцій керування колективними та індивідуальними перемиканнями, передавання сигналів у систему автоматизованого розподілу викликів, у блоки автоматичного збирання інформації, у блоки генерації вихідних дзвінків за попередніми переліками та в систему голосової пошти.

База даних комунікаційного сервера є ядром інформаційної системи. Функціонально базу даних може бути розбито на декілька основних баз:

- база даних клієнтів;
- предметна база даних з параметрами своєї установи;
- операційна база, де зберігаються алгоритми керування маршрутизацією запитів;
- статистична й агентська бази даних ЦОВ, куди записуються історія усіх подій та дії кожного агента при його спілкуванні з клієнтами; ведеться така статистика, котра допомагає оптимізувати роботу ЦОВ: завантаження обладнання, середня тривалість переговорів, час до зняття агентом трубки, кількість обслужених викликів, утомлюваність агента, його продуктивність; менеджери ЦОМ формують правила та сценарії обслуговування, контролюють продуктивність системи та роботу операторів;
- бібліотека прикладних програм API, котрі пишуться за допомогою спеціальних засобів із урахуванням змісту перших двох баз; API визначають

призначення та експлуатаційні можливості ЦОВ і мають постійно оновлюватись.

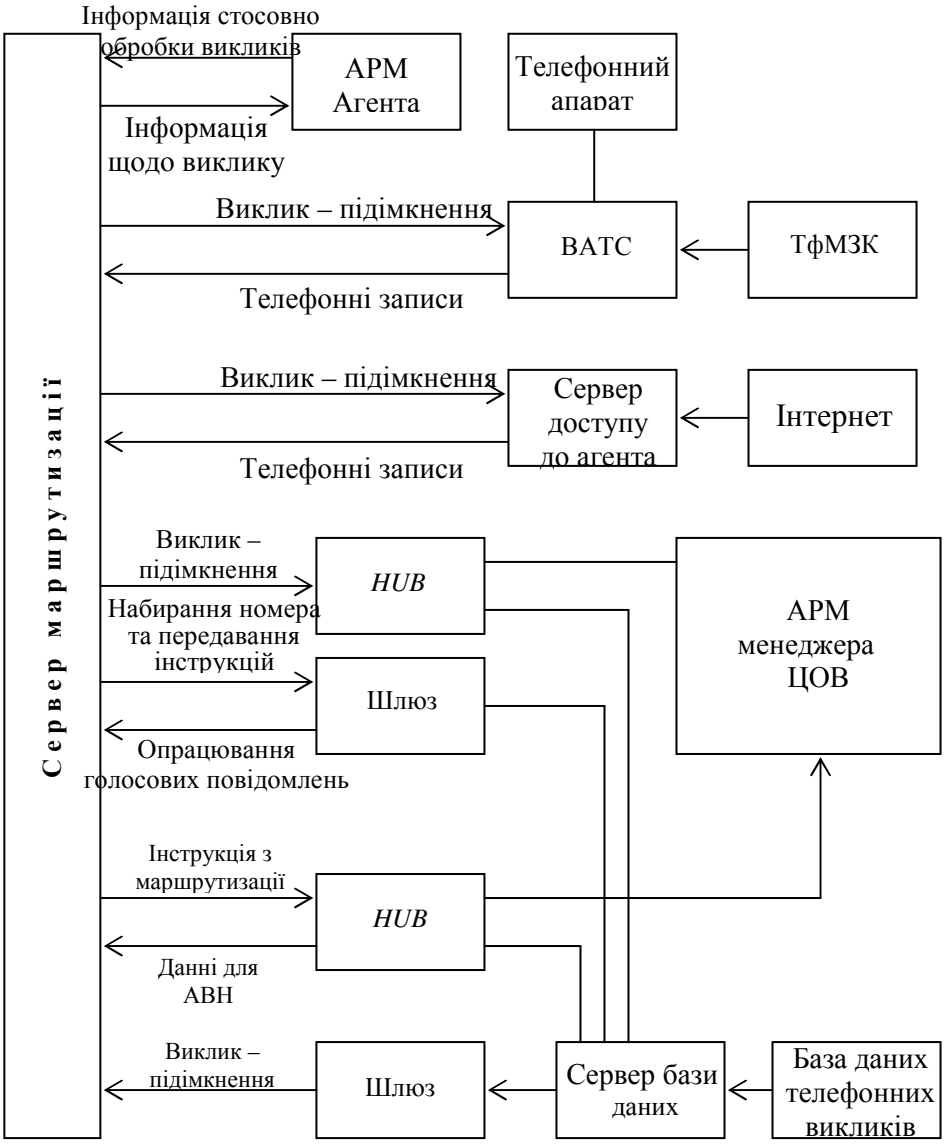

Рисунок – 6.3 Функціональна взаємодія апаратного та програмного забезпечення ЦОВ

HUB – це комутатори, які забезпечують з'єднання серверів та автоматизованих робочих місць (АРМ) для передавання сигналів виклику - підключення, набирання номера, інструкцій маршрутизації та з'єднання, даних для автоматичного визначення номера (АВН) тощо.

Система автоматичного дозвонювання є комплексом апаратури та ПЗ для автоматичної генерації вихідних викликів за заздалегідь підготовленими переліками. Алгоритм розсилання такий: якщо абонент відповідає на дзвінок, то він з'єднується з вільним агентом. Якщо ні, то дзвінок буде повторено пізніше. Частота викликів обчислюється залежно від завантаження ЦОВ.

Система інтерактивного голосового обміну є по суті автовідповідачем, котрий забезпечує систему голосового меню. Вибір пунктів меню споживач

здійснює за допомогою клавіатури звичайного телефону в режимі тонального набирання. Пристрій виконується у вигляді окремого блока і сполучається з АТС та комп'ютерною системою за стандартними протоколами (H.323 тощо).

Сервер баз даних може бути виділеним або функціонувати як ПЗ на комунікаційному сервері. Він організує доступ усіх частин ЦОВ до записів баз даних.

Сервер статистики забезпечує збирання інформації щодо роботи усього ЦОВ та окремих агентів.

6.2 Задачі та архітектура центру обробки викликів служби «Міліція» на базі відомчої ЦАТС»

Операторський центр обробки викликів служби «Міліція» може бути побудований як показано на рис. 6.3. Фізично виклики розподіляються по робочим місцям – консолям [24].

Консоль може бути реалізована різними способами, залежно від апаратно-програмних рішень, застосованих в устаткуванні в цілому. В ранніх системах СРВ (побудованих на базі УАТС) консоль складалася з двох різних складових: телефонної і комп'ютерної.

Телефонна частина консолі забезпечує прийом телефонних викликів і є пристроєм підтримки мовного діалогу «абонент-оператор». В найпростішому випадку - це аналоговий телефонний апарат з телефонною трубкою або гарнітурою, що підключається до системи по двох дротяних аналогових абонентних лініях. В деяких системах - це стандартний телефонний ISDN або спеціалізований апарат, забезпечений рідкокристалічним дисплеєм, світлодіодами для індикації виклику і функціональними клавішами, за допомогою яких проводяться всі основні операції, пов'язані з його обслуговуванням (прийом, переадресація, відбій і т. п.).

Комп'ютерна складова підтримує інтерфейс оператора із спеціалізованою базою даних служби «Міліція». В більшості побудованих на базі УАТС систем ці дві складові використовують для обміну інформацією принципово різні мережі і синхронізуються через управляючий сервер СРВ.

Введення інтерфейсу для зовнішнього управління алгоритмом обробки виклику (*Application Programming Interface*, *API)*, вивченню якого присвячено окреме заняття.

Головна перевага, яка досягається впровадженням API - функціональна розширюваність контакт-центру. Крім того, витягуючи і аналізуючи інформацію, зв'язану з викликом (номер викликаючого абонента, дані, одержані при діалозі з IVR і т. д.), і оперативно взаємодіючи з базами даних служби «Міліція», що підключаються через API, до моменту прийому власне телефонного виклику контакт-центр вже забезпечує оператора необхідною довідковою інформацією, що відноситься до цього виклику. Таким чином, вся інформація, супроводжуюча запит (номер телефону, ім'я, регіон мешкання, що цікавить питання, попередня історія і т. п.), прочитується з бази даних центру і з'являється на екрані робочого місця оператора (автоматично або по його команді). Ця функція економить робочий час

оператора, підвищує ефективність обслуговування викликів і виконання пов'язаних з ним задач.

Атрибути оператора служби «Міліція»:

- прізвище, ім'я, по батькові;
- звання;
- посада;
- реєстраційне ім'я;
- особистий ідентифікаційний номер;
- особистий пароль;

додаткові дані, що визначають права і кваліфікацію оператора.

Контроль і управління цими атрибутами покладається на керівника служби. Можливості, що надаються оператору, визначаються його правами і задачами, вирішуваними даним операторським центром.

У загальному випадку вони описуються наступним набором функцій:

- реєстрація в певній операторській групі;
- припинення реєстрації;
- короткочасне блокування консолі;
- прийом вхідних викликів з черги (персональної, черги групи, черги служби);
- переадресація виклику (до іншого оператора, до старшого оператора, до іншої групи операторів, до автоінформатора);
- примусове роз’єднання;
- утримання з'єднання з одночасним службовим викликом старшого оператора (для консультації);
- запис розмови з абонентом;
- прийом від системи вихідного з'єднання, наперед встановленого нею за списком сповіщення.

Оператор (контролер) служби «Міліція», має право не тільки займатися обслуговуванням викликів, що поступають від абонентів, але і контролювати роботу операторів в групі (підключаючись в режимі прихованого прослуховування і аналізуючи статистичну і оперативну інформацію).

Сповіщення про вхідний виклик може бути передано на робоче місце оператора двома способами:

- за допомогою візуальної індикації;
- тональним сигналом, посланим в гарнітуру оператора.

Статистика і облік викликів. Облік викликів, накопичення і аналіз статистичної інформації про роботу операторів є основним засобом оцінки ефективності функціонування служби «102». Накопичувану і контрольовану інформацію служби «Міліція» можна розділити на три основні категорії: оперативна, статистична, обліку викликів.

Оперативна інформація дозволяє керівництву служби «102» контролювати функціонування устаткування, оцінювати поточне завантаження служби тощо. До оперативної поточної інформації відносяться: завантаження розмовних каналів; довжина черг; стан операторських консолей і певного оператора.

Інформація обліку викликів включає параметри кожного виклику, прийнятого/обслугованого/втраченого службою «102», *статистичні дані* про які, як правило, нагромаджуються і аналізуються керівництвом служби. Тут враховуються: тип виклику (вхідний/вихідний/внутрішній); кількість викликів за певний проміжок часу; середня довжина черги (величина, потрібна для оптимізації числа операторів); середня тривалість розмови; співвідношення числа користувачів, обслужених за допомогою системи *IVR* і операторів; час, протягом якого всі лінії зайняті; середній час зайнятості оператора; середнє число операторів, що знаходяться в службі за певний проміжок часу; середній час утримання з'єднання; середня тривалість інтервалу між закінченням обслуговування виклику і початком обслуговування наступного виклику; максимальна тривалість очікування; не обслуговані виклики (абонент не дочекався відповіді оператора або не додзвонився унаслідок зайнятості всіх операторів і місць в черзі); середня інтенсивність повторних викликів; ідентифікаційний номер оператора, що обслужив виклик; номер групи операторів; відсоток обслугованих викликів.

Істотною вимогою до *Call* - центрів служби «102» є необхідність тісної інтеграції (і взаємодії в процесі обслуговування викликів) комутаційної підсистеми з інформаційними базами даних служби «Міліція» і із загальними міліційними інформаційними базами даних. Для обслуговування кожного виклику, будь він що вхідний або вихідний, потрібний доступ до даних, що зберігається у відповідних інформаційних базах центру, і, можливо, модифікація цих даних.

Сучасні *Call* - центри можуть мати сотні або тисячі операторів, які знаходяться в одному місці, або розміщених в декількох регіональних центрах, або розосереджених по всій країні. З технічної точки зору це означає наявність мережі СРВ (так званого віртуального *Call* – центру – системи розподілу викликів), зв'язаних між собою високошвидкісними каналами передачі даних (щоб забезпечувалася робота із загальними базами даних).

Існує цілий ряд способів реалізації такого універсального доступу. Одним з найперспективніших і економічно доцільних способів є доступ на базі технології *IP*-телефонії. Мовний діалог з користувачем проводиться у вигляді сеансу *VoIP* з використанням вже наявного з'єднання *Web*-сайту з Інтернет. При цьому користувач і оператор *Call* - центру можуть вести діалог і навіть синхронно проглядати одні і ті ж *Web*-сторінки (рис. 6.4).

При виклику із Інтернет користувач отримує доступ до *Cal l*- центру служби «Міліція» того чи іншого регіону, клацнувши мишкою на кнопку «*call*», яка знаходиться на її *Web*-сторінці, що активізує програму IP-телефонії, зареєстровану на *Web* - браузері. Ця програма може бути інтегрованим застосуванням *Web* - браузера чи окремим застосуванням, який викликається браузером із будь-якого місця на робочому столі користувача.

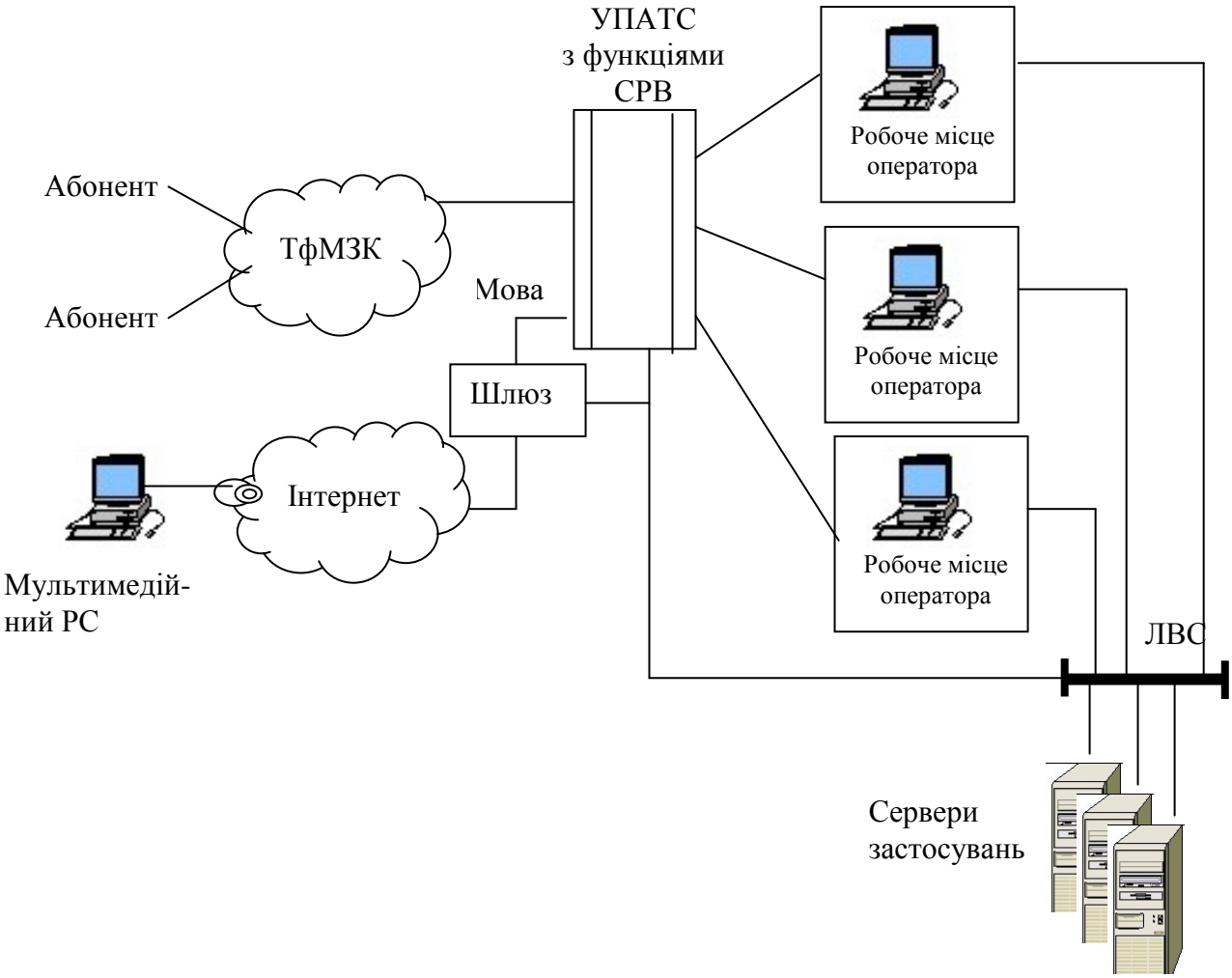

Рисунок 6.4 – Варіанти доступу до контакт-центру служби «Міліції»

Механізми обслуговування заявок можуть бути різними. Їх можуть обслуговувати або окремі оператори або групи операторів, або ті ж оператори, які обслуговують основний (мовний) потік запитів. Якщо другий варіант застосовний, з'являється можливість істотно збільшити продуктивність *Call* - центру, причому зробити це не за рахунок збільшення числа операторів, а за рахунок обробки запитів різних видів одним і тим же оператором. Запити, що допускають відкладену обробку, оператор може обробляти в періоди, коли інтенсивність потоку телефонних запитів знижується.

У типовому сценарії користувач передає повідомлення електронної пошти в центр обслуговування або по звичайному каналу електронної пошти, або шляхом заповнення форми на *Web*-сайті. Далі повідомлення проходить по Інтернет до поштового серверу, встановленого в приміщенні користувача. Після прибуття повідомлення на поштовий сервер операторського центру генерується віртуальний виклик. Цей віртуальний виклик призначений для передачі повідомлення оператору: він сприймається як звичайний телефонний виклик, ставиться в чергу і маршрутизується відповідно до алгоритму і набору засобів, визначеного управляючим застосуванням.

Коли звільняється оператор, здатний обслужити виклик цього типу і тематики, «виклик» електронної пошти поступає до терміналу оператора, і той одержує повідомлення про його присутність на екрані браузера. Коли звільняється оператор, здатний обслужити виклик цього типу і тематики, «виклик» електронної пошти поступає до терміналу оператора, і той одержує повідомлення про його присутність на екрані браузера. Призначений для користувача інтерфейс робочого місця оператора *Call*-центру містить ряд інструментальних засобів, за допомогою яких оператор має нагоду створити відповідь для передачі його по електронній пошті, пере вести «виклик» в режим утримання для наведення довідки у інших операторів *Call* - центру або переправити «виклик» іншому оператору, що вважається фахівцем в даній області. Під час виконання всіх цих дій оператор, зайнятий обслуговуванням виклику, що поступив у вигляді електронного листа, вважається зайнятим, і інші виклики поступати до його робочого місця не можуть.

6.3 Задачі та архітектура *IP* - контакт-центру служби «Міліція»

На відміну від «операторського центру» або «*Call* - центру», які оперують в основному з телефонними викликами, «Контакт центри» мають розширені функціональні можливості.

Перш за все, звичайно, це мультимедійність, що розуміється як здатність обслуговувати запити різних типів, що поступають з різних телекомунікаційних мереж:

- мовного зв’язку - з ТфМЗК;
- мовного зв’язку - з Інтернет, з використанням технології *IP*-телефонії;
- зв’язку факсом, електронною поштою;
- відеовиклики (в недалекій перспективі).

Мультимедійність починається з доступу до послуг контакт-центрів.

Розглянемо деякі із способів доступу до послуг, які характерні саме для контакт-центру, інтегрованого з *Web*. Як правило, інтегрований контакт-центр для декількох служб надає користувачу доступ до своїх ресурсів з боку *Web*-сайту чи пов'язаних з цим *Web*-сайтом операторів. Таким чином, задачею контакт-центру є забезпечення універсальності доступу з погляду абонента, свободи вибору методу доступу до послуг контакт-центру.

Наступний спосіб - режим текстового чату, доступу до послуг операторського центру з'явився саме в контакт-центрах. Такий спосіб дає можливість обміну текстовою інформацією між користувачем і оператором центру в реальному часі і може бути особливо актуальний у разі відсутності у користувача ПО і устаткування *VoIP* або незадовільної якості мови при використовуванні *IP*-телефонії, а також у випадках, коли треба безпомилково передати цифри, точне написання прізвищ і т.д.

Задачі, які повинні розв'язуватися контакт-центром служби «Міліція»:

- забезпечення широкого спектру можливостей як в плані доступу, так і з погляду послуг, що надаються з використанням людських ресурсів (операторів) і автоматизованих систем;

- гарантована обробка транзакцій всіх типів незалежно від джерела виклику і методу доступу до ресурсів контакт-центру;

- забезпечення можливості інтеграції з існуючими операторськими центрами і до оснащення їх необхідними функціями із застосуванням устаткування сторонніх виробників за рахунок використовування відкритих стандартів при побудові систем.

Технології пакетної комутації дозволяють у принципі відмовитися від громіздкого комутатора каналів, поклавши функції комутації на саму мережу з використанням можливостей протоколу *IP* як універсального транспортного протоколу. В цьому випадку функції комутації розмовних каналів зводяться до управління медіапотоками між певними вузлами комп'ютерної мережі. Всі функціональні можливості реалізуються комп'ютерними серверами застосувань, що працюють з управляючою інформацією і медіапотоками (якщо необхідно) і взаємодіючими в процесі обслуговування виклику з інформаційними і технологічними базами даних. При цьому кожний з таких серверів відповідає за свій набір послуг (CPB, *IVR* і ін.). Таким же чином розв'язуються питання надійності (стандартні методи резервування апаратного забезпечення комп'ютерної техніки), масштабування (установка, при необхідності, серверів застосувань, що працюють в режимі розділення навантаження), введення нових функцій (додаткові сервери і застосування), створення розподілених систем (достатньо зв'язати різні офіси однією комп'ютерною мережею, що володіє потрібною пропускною спроможністю).

Ядром систем такого роду є програмний продукт, що управляє чергами і маршрутизацією викликів. До складу системи входять також периферійні шлюзи, що забезпечують взаємодію компонентів системи, прийом і обробку викликів, що поступають з різних мереж, сервери застосувань і баз даних, функції яких будуть розглянуті нижче.

Використання *IP*-технологій дозволяє легко пов'язати телефонний виклик з інформацією про нього. Цей зв'язок надзвичайно важливий для контакт-центрів, саме він робить ефективною обробку викликів з різних середовищ і забезпечує необхідну якість обслуговування. Якщо взяти до уваги і інші переваги *IP* – контакт - центрів, у тому числі низьку вартість розгортання і ефективність масштабування, привабливість використовування в контакт-центрах пакетної комутації стає очевидною.

В той же час віртуальна природа *IP*-адресації в сучасних контакт-центрах дозволяє легко розв'язати ці проблеми (рис. 6.5) Оператор може реєструватися на будь-якому терміналі і при цьому він буде розпізнаний системою як унікальний агент, що володіє певною кваліфікацією.

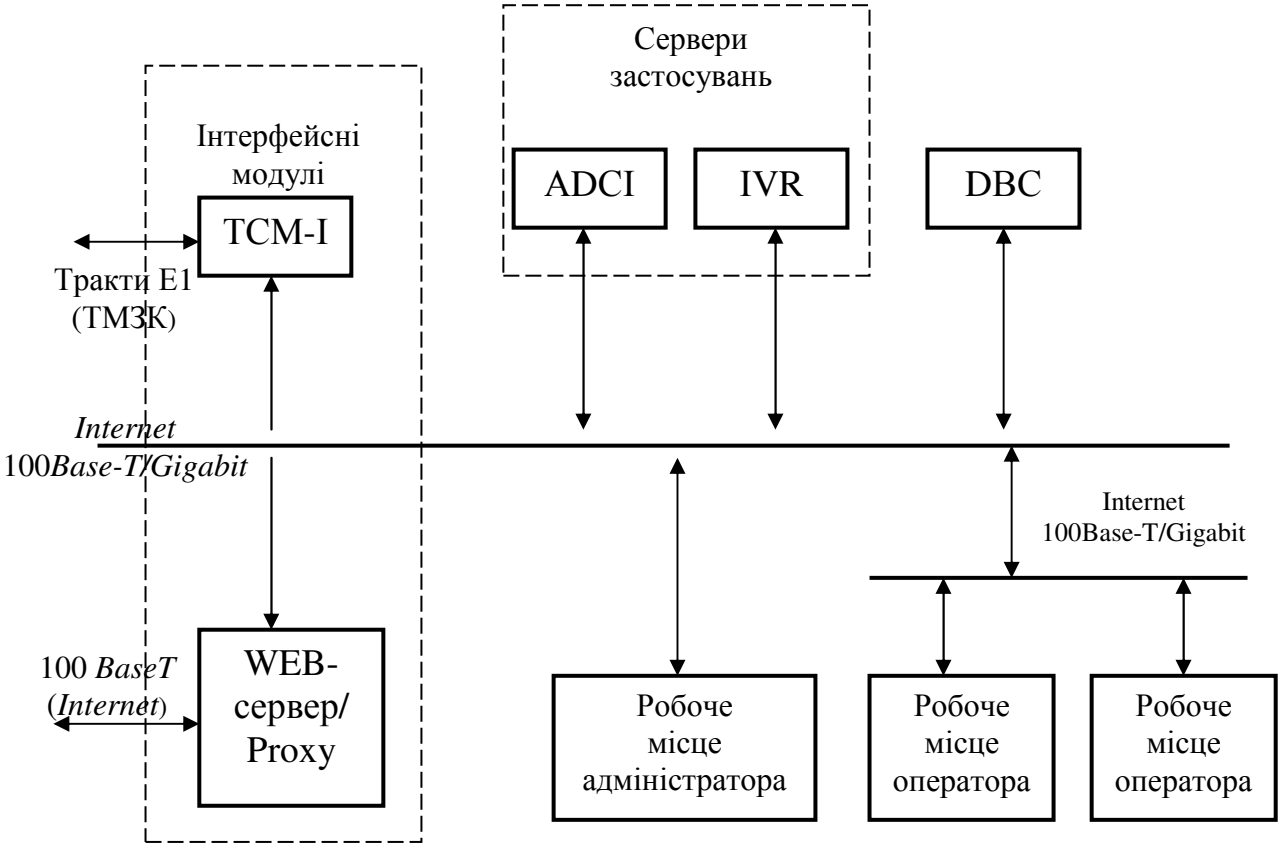

Рисунок 6.5 – Типова структура *IP* – контакт - центра служби «102»

Очевидні переваги контакт-центру з погляду витрат на організацію видалених робочих місць. Розглянемо функції блоків (рис. 6.5).

6.3.1.Шлюз IP-телефонії

Шлюз *IP*-телефонії забезпечує взаємодію між мережею з комутацією пакетів *IP* і телефонною мережею з комутацією каналів. Шлюз є програмно-апаратним комплексом, основним функціональним призначенням якого є перетворення мовної інформації, що поступає з боку ТфМЗК, у вигляд, придатний для передачі по мережах з маршрутизацією пакетів *IP*: кодування і упаковка мовної інформації в пакети *RTP*/*UDP*/*IP*, а також зворотне перетворення. Ще одна функція шлюзу - перетворення номера ТфМЗК в *IP*-адресу - реалізується в шлюзах для роботи в мережі *IP*-телефонії без сторожа. Крім того, шлюз підтримує обмін сигнальними повідомленнями як з вузлами комутації/термінальним устаткуванням ТфМЗК, так і з пристроями, що працюють за стандартами *IP*-телефонії H.323 чи *SIP*.

Як правило, при використовуванні *IVR* алгоритми обробки викликів в операторському центрі передбачають передачу абонентам, чекаючим в черзі, аудіоінформації, наприклад, мовних фраз. Ці фрази можуть містити відомості про порядковий номер виклику в черзі і орієнтовному часі очікування. Крім того, цілком можливо, що, прослуховуючи такі фрази, абонент одержить потрібну йому інформацію автоматично.

6.3.2.Сервери застосувань

Сервери застосувань забезпечують реалізацію логіки послуг, що надаються. Стосовно операторських центрів можна виділити два базові типи застосувань, які повинні підтримуватися для того, щоб система була повно функціональною і задовольняла вимогам, про які мовилося вище: інтерактивна мовна взаємодія і розподіл викликів.

Сервер інтерактивної мовної взаємодії *IVR* виконує всі функції, пов'язані з організацією комп'ютерного діалогу з абонентом, який звернувся в контакт-центр. Це і передача абоненту мовних підказок-запрошень, і прийом від абонента додаткової інформації в режимі багаточастотного донабору, і передача абоненту в автоматичному режимі різного роду довідкової і сервісної інформації, і підтримка функцій синтезу мови, і багато інших функції, реалізовувані сучасними *IVR*, які детально розглядалися раніше.

Сервер розподілу викликів СРВ є ключовим елементом контакт-центру. Динамічно взаємодіючи з базами даних в процесі обслуговування викликів, він забезпечує підтримку систем черг і функцій маршрутизації викликів, що надходять до контакт-центру.

6.3.3.Бази даних

Бази даних операторського центру зберігають інформацію про конфігурації системи, статистичні дані її функціонування і обліку і, можливо, ситуаційних карт і т.д.

6.3.4.Сервер експлуатаційного управління

Сервер/термінал експлуатаційного управління фактично є звичайним персональним комп'ютером (робоче місце адміністратора системи) із спеціалізованим програмним забезпеченням. З його допомогою виконуються функції конфігурації і діагностики системи, контроль стану інтерфейсів і розмовних каналів, збір оперативної і статистичної інформації про роботу системи і обслуговування викликів, а також генерація звітів і архівація.

6.3.5.Робочі місця операторів

Консолі операторів організовуються на базі стандартних персональних комп'ютерів зі встановленим спеціалізованим клієнтським програмним забезпеченням (або Web-браузером). Якщо в операторському центрі використовується повністю інтегроване рішення на базі протоколу *IP*, то робоче місце оператора оснащується мультимедійними засобами - спеціальною гарнітурою і т.д. Мовна інформація в цьому випадку передається в пакетному вигляді з використанням кодування G.711 або G.729.

Управління даними - здатність системи збирати, сортувати і зберігати інформацію про користувачів, яка використовується для маршрутизації викликів до самого відповідного оператора центру. Незалежно від того, в якій формі поступає запит, вся інформація, що відноситься до даного виклику, збирається і зберігається в базі даних.

6.4 Алгоритми обслуговування викликів та можливості контакт-центру служби «Міліція»

Контакт-центри обслуговування викликів працюють як системи обслуговування з очікуванням. За відсутності вільних операторів в групі, що мають нагоду кваліфіковано обробити запит, виклик поміщається в чергу. В якості опції передбачається видача абоненту під час знаходження виклику в черзі різного роду інформації, а також інформування абонента про порядковий номер в черзі і приблизному часі очікування.

Після того, як абонент набрав номер служби, що викликається, (наприклад, «102»), виклик прямує на сервер розподілу викликів (*ACD*), який може діяти за наступними сценаріями:

- виклик прямує безпосередньо на робоче місце оператора, у разі наявності вільних операторів в групі, з використанням встановленого для цієї служби алгоритму розподілу;
- виклик прямує в чергу у випадку, якщо немає вільних операторів;
- виклик може прямувати на систему *IVR*, після чого адресується безпосередньо на робоче місце оператора (у разі потреби), якщо МЦОВ оснащений відповідними програмно-апаратними опціями;
- виклик прямує на систему *IVR*, після чого відбувається постановка в необхідну чергу у випадку, якщо у відповідній групі (службі) немає вільних операторів;
- у разі відсутності вільних операторів і місць в черзі очікування здійснюється роз'єднання.

Маршрутизація викликів в необхідну групу операторів здійснюється на підставі набраного номера служби або інформації АОН.

6.4.1.Алгоритм обслуговування вхідного виклику за технологією VoIP

Посилення ролі Internet як засобу доступу до інформації обумовлює необхідність наявності в архітектурі будь-якого сучасного операторського центру Web-серверу, через який користувачі операторського центру можуть отримувати доступ до послуг через мережу Інтернет.

Абонент, охочий одержати необхідну інформацію, використовуючи ресурси контакт-центру про які-небудь документи (паспортний стіл тощо), в процесі перегляду *Web*-сторінки компанії активізує відповідну іконку. При активізації починається процедура виклику через Інтернет до шлюзу *IP*-телефонії, через вже встановлене з'єднання з інтернет-провайдером. Шлюз *IP*-телефонії завантажує Java-додаток обробки виклику в комп’ютер користувача для запуску

застосування *IP*-телефонії. *Java*-застосування забезпечує інтерфейс, через який користувач може також одержувати повідомлення про стан виклику, брати участь в обміні текстовими повідомленнями або роз'єднати виклик. Виклик, створюваний з використанням технології *VoIP*, обслуговується системою повністю, аналогічно виклику, що поступає з телефонної мережі.

6.4.2.Алгоритм обслуговування виклику в режимі «Call-back»

Режим відкладеного обслуговування передбачає постановку виклику в чергу на обслуговування, без необхідності його утримання з подальшим зворотним викликом вільного оператора до абонента. Абонент може замовити зворотний виклик з інформаційного сайту служби «Міліція», наприклад, паспортного столу.

При замовленні зворотного виклику з *Web*-сайту передбачається заповнення абонентом відповідної форми з вказівкою орієнтовного часу, способу зв'язку і контактного телефону. Сформована заявка на зворотний виклик ставиться в чергу і далі обслуговується відповідно до алгоритму обслуговування вихідного виклику.

6.4.3.Алгоритм обслуговування виклику по електронній пошті

Абонент може дістати доступ до оператора служби «Міліція» з використанням електронної пошти. Всі виклики з однаковим пріоритетом прямують на робочий стіл оператора системи. Таким чином забезпечується ефективна обробка всіх видів трафіку, що проходить через систему.

6.4.4.Алгоритм обслуговування вихідного виклику

У системі МЦОВ передбачена наявність можливості попереджуючого набору номера. Подібна функція необхідна у випадку, якщо в процесі функціонування системи потрібна організація вихідного трафіку (наприклад, для реалізації алгоритму обслуговування абонентів по системі із зворотним викликом). У такому разі система або сама генерує список обдзвону абонентів, або цей список формується силами персоналу центру обслуговування викликів.

Система автоматично виконує виклики по сформованим активним спискам сповіщення, визначає стан номера викликаємого абонента (Зайнято; Невідповідь; Факс; «Жива» відповідь). При розпізнаванні відповіді здійснюється проключення виклику на вільного оператора (з можливістю попередньої передачі абоненту необхідної фрази авто інформатора).

6.4.5.Алгоритм розподілу викликів по оператора

Алгоритм роботи системи МЦОВ забезпечує розподіл викликів між операторами служби «Міліція» таким чином, що навантаження на кожного з них завжди залишається однаковим.

Для рівномірного розподілу навантаження серед операторів використовуються три основні алгоритми:

- циклічний розподіл викликів, тобто на першого вільного оператора;
- вибір найбільш вільного оператора (після обслуговування останнього виклику), тобто вибір оператора, якому буде направлений виклик з черги, здійснюється з урахуванням двох параметрів: вільного від обслуговування користувачів часу і рівня кваліфікації оператора;
- вибір якнайменше зайнятого оператора (з початку зміни), тобто виклик з черги прямує на оператора, що характеризується якнайменшим навантаженням. В якості критерію вибору використовується або загальний сумарний час розмов оператора, або загальна кількість викликів, обслужених даним оператором. Передбачена модифікація даного алгоритму з можливістю обліку коефіцієнта кваліфікації оператора.

Це позитивно позначається на якості роботи персоналу центру і дозволяє новим співробітникам швидше набиратися досвіду. Алгоритми розподілу викликів, вживані в системі, підтримують можливість розділення операторів по кваліфікації, що дозволяє ефективно здійснювати обробку заявок. Крім того, система може бути гнучко набудована під конкретні вимоги замовника.

6.4.6.Можливості операторів в системі

У системі передбачена організація декількох груп операторів служби «Міліція». В групі може бути одне або декілька робочих місць операторів. Оператори в системі ідентифікуються унікальним номером (ім'ям) і мають свій пароль. Підтримується розділення на операторів і старших операторів, які володіють різними правами доступу.

Оператору центру надаються наступні можливості:

- реєстрація в необхідній групі на будь-якому робочому місці під унікальним паролем;
- прийом вхідних викликів з ТфМЗК;
- організація вихідних викликів;
- утримання виклику;
- консультація (другий виклик);
- переадресація виклику в іншу групу/службу/на старшого оператора;
- короткочасний вихід з режиму обслуговування викликів (блокування консолі);
- примусове роз'єднання виклику;
- звернення до бази даних центру в процесі обслуговування виклику;
- запис переговорів з абонентами.

Під час надходження вхідного виклику на робочому місці оператора (на екрані ПК) відображається інформація про викликаючого абонента. Забезпечується можливість регістрації заявки, що надійшла, шляхом заповнення «ситуаційної карти» з використанням технології взпливаючого вікна.

Відомості про дзвонячого:

- номер викликаючого абонента;

- адреса, по якій зареєстрований телефон;
- у випадку якщо телефон домашній:
- ФІО (і можливо паспортні дані) абонента, на якого зареєстрований номер;
- список осіб, зареєстрованих за даною адресою, наявність у них зброї, судимості, транспорту.

Відомості про подію: *I*

- адреса, де вчинено правопорушення;
- ФІО всіх громадян, прописаних за цією адресою;
- наявність судимості і зброї; транспорт.

6.4.7. Можливості старшого оператора

1. Старший оператор служби «Міліція» має нагоду контролювати процес прийому і обслуговування викликів, для чого йому надається наступна інформація:

стан операторів в своїй службі/групі;

стан черги;

статистика по вибраному оператору (кількість обслужених викликів, час, протягом якого був зайнятий оператор і т. д.).

2. Для контролю роботи операторів своєї групи старшому оператору доступні наступні функції:

блокування/розблокування оператора;

виклик оператора;

підключення до розмови оператора з абонентом;

запис переговорів операторів з абонентами з можливістю подальшого прослуховування з комп'ютера старшого оператора. Функція запису розмови доступна також звичному агенту.

3. У системі передбачена можливість одночасного запису розмов декількох операторів.

4. Старший оператор має нагоду переміщати і видаляти виклики з черги.

5. Додатково старшому оператору доступні всі можливості звичайного оператора.

6.4.8.Режими обслуговування викликів

Система МЦОВ підтримує наступні режими обслуговування викликів: передвідповідь, відповідь .Режим обслуговування задається індивідуально для кожної групи.

6.4.9.Маршрутизація викликів

Система МЦОВ підтримує можливість гнучкої маршрутизації викликів. Виклик може прямувати в ту або іншу групу операторів по різних критеріях: набраний номер, інформація АОН тощо.

Залежно від різних параметрів, що задаються адміністратором системи, виклики можуть маршрутизуватися до різних операторських груп і до різних операторів, абоненти можуть одержувати різну інформацію тощо.

Передбачені наступні основні критерії маршрутизації викликів:

- набраний номер;
- інформація АОН;
- число викликів, що чекають в черзі до даної групи операторів;
- кваліфікація оператора;
- кількість операторів в групі, здатних обслужити заявку;
- алгоритм розподілу викликів.

Завдяки комбінації даних параметрів, можна розробити гнучкі алгоритми обслуговування викликів.

Для оптимізації роботи центру обслуговування викликів і більш рівномірного завантаження операторів в системі передбачені гнучкі алгоритми маршрутизації. Настройка того або іншого алгоритму здійснюється на основі аналізу цілей і параметрів упровадження МЦОВ.

6.4.10. Збір статистичної інформації і облік викликів

У системі передбачено формування, зберігання обширної статистичної і експлуатаційної інформації, а також можливість генерації звітів реального часу і хронологічних довгострокових звітів.

Інформацію в системі можна розділити на накопичувану в базі даних по кожному конкретному клієнту, що звертається (дзвонить) на службу і накопичувану в процесі обліку викликів.

У системі передбачена можливість генерації звітів (за узгодженням із замовником). Можлива генерація звітів реального часу і хронологічних довгострокових звітів. Звіти формуються по запитах з робочого місця адміністратора системи. Генерація звітів може проводитися по годинні, добі, тижням і т.д.

Можливий збір різноманітної статистичної інформації по конкретному дзвонячому, наприклад:

- номер абонента, що викликається;
- характер попередніх запитів;
- дата першого звернення тощо.

Під час надходження виклику на робочому місці оператора забезпечується можливість автоматичної появи всієї оперативної інформації по абоненту, що викликається.

Під час надходження виклику фіксується наступна інформація:

- тип виклику;
- час надходження виклику;
- номер, категорія абонента, що викликається;
- номер абонента, що викликає;
- час завершення сеансу зв'язку;
- тривалість очікування обслуговування;

- тривалість розмови;
- номер оператора, що обслужив виклик;
- статус виклику (обслуговований/втрачений);
- етап обслуговування, на якому виклик був втрачений (для втрачених викликів);
- ініціатор відбою;
- при необхідності створюється ситуаційна карта.

У режимі реального часу передбачена видача наступних типів звітів:
- стан всіх операторів в групі;
- стан всіх робочих місць МЦОВ;
- стан черг до кожної групи операторів.

Крім того, в реальному масштабі часу старший оператор має нагоду одержати інформацію за часом очікування викликів в черзі, середній тривалості розмови і т.д.

Система генерує наступні типи хронологічних звітів:
- інформація по кількості будь-якого типу викликів, що пройшли через систему (вхідний/внутрішній/вихідний) за будь-який проміжок часу;
- інформація по статусу викликів: скільки за певний проміжок часу викликів було обслужено/втрачено/не обслуговано;
- кількість викликів, втрачених до граничного часу очікування обслуговування;
- кількість викликів, втрачених після граничного часу очікування обслуговування;
- кількість викликів, оброблених одним оператором за будь-який проміжок часу;
- кількість викликів, оброблених всіма операторами групи/служби сумарно за будь-який проміжок часу;
- сумарна зайнятість одного/всіх операторів за робочу зміну (за часом);
- кількість переадресацій унаслідок зайнятості всіх операторів за будь-який проміжок часу;
- розподіл часу оператора на обробку різних типів викликів.

Забезпечуються генерація звітів по годинам, добі, тижням, місяцям, кварталам, зберігання в базі даних МЦОВ архівної інформації про встановлених з'єднаннях, а також статистичній інформації за період 8 мес, об'єм БД може бути збільшений за узгодженням із замовником.

6.4.11.Адміністрування

Надійне функціонування контакт-центру служби «Міліція» неможливе без підсистеми адміністрування, здатної забезпечити швидке реагування на зміни, що впливають на роботу контакт-центра, а значить, що відбиваються і на якості обслуговування абонентів. Необхідно постійно контролювати роботу центру, змінюючи, коли потрібно, число операторів в тій або іншій групі, створюючи нові напрями, модифікуючи алгоритми обслуговування і тощо, для чого в

контакт-центрі є спеціалізована підсистема звітності і адміністративного управління.

Разом з операторами і старшими операторами в системі передбачена наявність адміністратора, на якого покладені функції управління роботою системи.

Основні функції адміністратора системи:

- закріплення повних і скорочених номерів доступу за службами (групами операторів); :
- управління атрибутами оператора (параметри реєстрації (номер облікового запису, пароль); визначення робочого місця (місць) для оператора; визначення приналежності оператора до групи (групам) тощо);
- управління кількістю і атрибутами груп операторів (визначення складу операторів, що входять до групи; завдання пріоритету групи і т. д.);
- управління роботою групи операторів (блокування/розблокування робочої групи);
- настройка режиму обслуговування вхідних викликів (відповідь/перед відповідь);
- управління переадресацією вхідних викликів;
- настройка критеріїв маршрутизації викликів;
- настройка алгоритмів розподілу викликів;
- управління автоінформаційними повідомленнями, необхідними для організації діалогу IVR з абонентом і іншими голосовими підказками;
- настройка параметрів інтерфейсу з опорною АТС;
- настройка «чорних списків» абонентів, яким заборонено обслуговування в системі.

6.5 Розрахунок якості обслуговування та кількості операторів

Характеристики доставки інформації та послуг користувачам в узагальненому вигляді входять в показники доступності і, частково, в показники конфіденційності і цілісності інформації [25]. Кількісна або якісна недостатність компонентів ЦОВ впливає на показники ефективності захисту інформаційних ресурсів. Кількість операторів (агентів) має відповідати заданому рівню обслуговування клієнтів ЦОВ. Виникає необхідність обчислення та контролю кількості агентів залежно від навантаження.

У даному разі може бути реалізовано дисципліну обслуговування як з відмовами, так і з очікуванням. Припустімо, що навантаження центру становить 250 викликів за 3,5 хв., а середня тривалість виклику – 20 с. Знайдемо залежність рівня обслуговування клієнтів від кількості операторів. Математично цю задачу розв’язав датський математик Ангер Крарупп Ерланг для випадку обчислення кількості телефоністок на телефонній станції з ручною комутацією. Практичні формули для проведення обчислень отримують, розглядаючи модель системи масового обслуговування з випадковим потоком запитів.

Випадкові потоки описуються функцією густини розподілу інтервалу між надходженнями двох подій $f(\Delta t)$, де випадкова величина $\Delta t = t_{i+1} - t_i$ для будь-яких i. Широко застосовується модель найпростішого потоку

$$f(\Delta t) = \lambda \exp(-\lambda \Delta t), \tag{6.1}$$

де λ – інтенсивність потоку.

Математичне сподівання довжини інтервалів між двома послідовними моментами надходження заявок $M[\Delta t] = 1/\lambda$. Ймовірність появи коротких інтервалів між двома послідовними запитами, довжина яких є менша за $M[\Delta t] = 0.63$. Це означає, що при найпростішому потоці короткі інтервали є частіші, аніж довгі. Найпростіший потік задає важчий режим роботи, аніж інші моделі потоків.

Випадкова подія на вході системи, запит або виклик характеризуються поряд з іншим двома параметрами: часом надходження і тривалістю обслуговування. Інтенсивність надходження (середня швидкість надходження), помножену на середню тривалість обслуговування, називають навантаженням: $a = \lambda h$. Інтенсивність навантаження є безрозмірною величиною, яку називають Ерлангом. Одним з фізичних тлумачень є те, що інтенсивність навантаження, виражена у Ерлангах, характеризує середню ефективність використання системи. При цьому 1 Ерл – це одне годинно-займання лінії за годину.

У тих випадках, коли абонентський термінал є цифровий і використовує пакетне передавання, загальне навантаження подають кількістю бітів, які проходять через лінію. Цей трафік можна подати як помноження тривалості пакетів на кількість пакетів кожного типу:

$$Y(d) = \sum_{i=1}^{m} \sum_{j=1}^{T} t_j n_{ij}(d), \tag{6.2}$$

де $n_{ij}(d)$ – середня кількість пакетів типу j у фазі i; t_j – тривалість пакета; i – фаза запиту; m – кількість фаз; j – тип пакета.

Основна модель надходження запитів (викликів): запити надходять від джерела з нескінченною кількістю запитів з розподілом Пуассона, а час обслуговування розподілено згідно з показовим законом [26]. Розподіл Пуассона подає ймовірність надходження i запитів протягом інтервалу часу t:

$$A(i,t) = \frac{(\lambda t)^i}{i!} e^{-\lambda t}, \tag{6.3}$$

де λ – інтенсивність надходження заявок й, водночас, середнє значення.

Розподіл за показовим законом має вигляд ймовірності обслуговування запитів протягом інтервалу часу, більшого за t, і задається рівнянням

$$H(>t) = e^{-\mu t}, \tag{6.4}$$

причому $h = 1/\mu$ є середнім значенням часу обслуговування.

Розподіл Пуассона є дискретним, тоді як розподіл (4) – неперервний. Знайдено, що сума M незалежних, ординарних, стаціонарних потоків з інтенсивностями λ_i ($I = 1, \ldots, M$) збігається до найпростішого потоку з інтенсивністю

$$\lambda = \sum_{i=1}^{N} \lambda_i \tag{6.5}$$

за умови, що доданки справляють однаково малий вплив на сумарний потік. Можна вважати, що за $N = 4...5$ сумарний потік є близький до найпростішого.

Для обчислення кількісних характеристик ЦОВ необхідно якомога точніше спрогнозувати середню кількість викликів за одиницю часу, визначити час найбільшого навантаження та опрацювати усі сценарії взаємодії з клієнтами, роботи автоматизованих систем відповіді і власне агентів. На підставі сценаріїв потрібно визначити середню тривалість кожного виклику та середній час зайнятості агента при обробці одного виклику. Після цього, на підставі отриманої інформації можна визначити кількість необхідних телефонних ліній, кількість агентів і натомість графік їхньої роботи.

При розв'язанні цієї задачі будемо враховувати, приміром, такі вимоги:

- жоден виклик не може бути втрачено; це означає, що необхідно зреалізувати дисципліну обслуговування з очікуванням та правильно обрати якісні показники обслуговування;
- час очікування сполучення клієнта з агентом має бути мінімальним; для абонента час очікування має бути майже непомітним або принаймні прийнятним;
- потрібен контроль за роботою агентів;
- необхідно автоматизувати оплату послуг, а отже, потрібна система обліку вартості для надання платних консультацій та довідок;
- центр має обробляти 2 000 викликів на добу, у тому числі 180 викликів у час найбільшого навантаження (ЧНН);
- середня тривалість обслуговування виклику $h = 1/\mu = 3$ хв. Отже, інтенсивність навантаження становить величину $a = \lambda/\mu = 180 \cdot 3/60 = 9$ Ерл.

Розглянемо для порівняння різні дисципліни обслуговування.

Системи масового обслуговування поділяються на дві категорії: системи з блокуванням та системи з очікуванням. Системи комутації каналів, як правило, належать до систем з блокуванням, а системи з пакетною комутацією – до систем з очікуванням. У моделі системи з блокуванням з n обслуговуючими пристроями запит обслуговується, якщо є хоча б один вільний доступний пристрій, і полишає систему, якщо всі обслуговуючі пристрої зайнято. Ймовірність блокування запиту задається відомою формулою Ерланга першого роду, що добре табульована [27]:

$$p(n) = \frac{a^n / n!}{\sum_{v=0}^{n} a^v / v!}. \qquad (6.6)$$

У моделі обслуговування з очікуванням з n обслуговуючими пристроями запит обслуговується, якщо є вільний пристрій і ставиться в чергу, якщо відсутні вільні обслуговуючі пристрої. Ймовірність того, що запит повинен очікувати, задається формулою Ерланга другого роду:

$$P(>0) = \left(\frac{a^n}{n!} \frac{n}{n-a} \right) : \left[\sum_{v=0}^{n-1} \frac{a^v}{v!} + \frac{a^n}{n!} \frac{n}{n-a} \right]. \qquad (6.7)$$

Якщо запити обслуговуються в порядку надходження, то ймовірність того, що запит має очікувати час, більший за *t,* є

$$P(>t) = P(>0)e^{-\mu(n-a)t}, \tag{6.8}$$

а середній час очікування становить величину

$$T = P(>0)/(\mu(n-a)). \tag{6.9}$$

Проведемо обчислення кількості агентів, необхідних для обслуговування запитів за різних систем обслуговування. Нехай у системі з блокуванням необхідно забезпечити якість обслуговування таку, щоби ймовірність блокування запиту була не більша за 0,005. Тоді на підставі рівняння (4) за допомогою таблиць, графіків або програми обчислень знаходимо, що при навантаженні 9 Ерл на ЦОВ необхідно мати в ЧНН 17 операторів. Обчислимо кількість операторів у системі з очікуванням, якщо якість обслуговування характеризується ймовірністю очікування протягом більше однієї хвилини і становить величину не більшу за ті самі 0,005. Для цього необхідно розв'язати рівняння (9) відносно *n*. Графічним способом знаходимо *n*, за якого задовольняється рівняння

$$P(>0) = T\mu(n-a) = 1/3(n-9).$$

Маємо в результаті 12 операторів.

Отже, системи з очікуванням забезпечують більш високе використання обладнання.

На відміну від традиційних телефонних систем, котрі описуються показовим розподілом часу обслуговування, у системах пакетного передавання більшість блоків даних або пакетів мають постійну довжину. У цьому випадку використовують розподіл Ерланга порядку *f*. Модель системи виглядає таким чином. Нехай обслуговування закінчується, коли промине декілька випадкових етапів. Наприклад, у системі ЦОВ відбудеться опитування абонента, звертання до бази даних, контроль рахунку абонента тощо. Якщо ці випадкові події описуються розподілом Пуассона з середнім значенням $f\mu$, то густина розподілу ймовірностей того, що запит буде обслуговано за час *t*, матиме вигляд функції

$$h(t) = \frac{(f\mu t)^{f-1}}{(f-1)!} e^{-f\mu t} f\mu. \tag{6.10}$$

При $f = 1$ маємо показовий закон розподілу, а випадок $f = \infty$ відповідає постійному часові обслуговування.

Детальні математичні рішення знайдено для систем масового обслуговування з очікуванням, котрі мають один обслуговуючий пристрій. Така модель є характерна для систем з використанням ЕОМ як централізованого керуючого пристрою. Розглядається модель, в якій запити надходять від джерела з нескінченно великою кількістю з інтенсивністю λ у єдиний обслуговуючий пристрій з довільним розподіленим *h(t)* часом обслуговування за середнього значення $1/\mu$ та дисперсії $\sigma^2 = 1/\mu^2 f$. Тоді середня кількість запитів, які очікують та перебувають на обслуговуванні, визначається за формулою Полячека – Хінчина

$$L = a + (a^2 + \lambda^2\sigma^2)/2(1-a), \tag{6.11}$$

де $a = \lambda\mu$.

Середня довжина черги обчислюється як

$$L_ч = a + (a^2 + \lambda^2\sigma^2)/2(1 - a), \quad (6.12)$$

а середній час очікування як

$$W = (a^2 + \lambda^2\sigma^2)/2\lambda(1 - a). \quad (6.13)$$

Якщо час обслуговування має показовий розподіл, то

$$L = a/(1 - a);\ W = a/\mu(1 - a). \quad (6.14)$$

А якщо час обслуговування постійний, то

$$L = (2 - a)/2(1 - a);\ W = a/2\mu(1 - a). \quad (6.15)$$

Як бачимо, за постійного часу обслуговування середній час очікування є у двічі меншим.

Моделі реальних мереж можуть бути надто складними. Тому для обчислень їхніх кількісних характеристик широко застосовується моделювання на ЕОМ. Високий рівень сучасних технологій дозволяє керувати якістю обслуговування під час технічної експлуатації ЦОВ. У статистичній базі зберігаються записи щодо історії всіх подій ЦОВ, проходження дзвінків, дій операторів, спілкування з клієнтами, різні статистичні параметри. За цими даними відображається оперативна статистика реального часу і складаються сукупні звіти. Наявність різноманітної статистичної інформації та звітів, доступних у реальному часі, дозволяє здійснювати оперативне керування обслуговуванням викликів, прогнозувати час очікування обслуговування, гнучко перерозподіляти дзвінки, збалансовувати навантаження операторів, коригувати поточну конфігурацію та оптимізувати роботу системи.

6.6 Вимоги до технічного захисту інформації в органах внутрішніх справ

Політика інформаційної безпеки центру обробки викликів і контакт-центру повинна бути частиною політики інформаційної безпеки органу внутрішніх справ і бути взаємно узгодженими. Розглянемо загрози і вимоги зо системи інформаційної безпеки органу внутрішніх справ.

Загрози інформаційної безпеки. Виникаючі в процесі діяльності органу внутрішніх справ загрози розділяються по характеру джерела на два базові класи - зовнішні і внутрішні. До першого відносяться наступні види загроз:

а) загрози фізичного проникнення сторонніх осіб з метою розкрадання критичної інформації на різних носіях;

б) загрози проникнення в корпоративну мережу з метою отримання разового або постійного доступу до критичної інформації;

в) загрози різних зовнішніх дій на корпоративну мережу з метою дезорганізації її роботи, нанесення матеріального збитку різноманітними способами;

г) загрози упровадження в корпоративну мережу ззовні з метою використання її ресурсів в особистих цілях;

д) загрози зняття інформації з працюючих комп'ютерів шляхом візуального спостереження і сканування їх електромагнітних або сонарних сигнатур.

До другого класу відносяться наступні види загроз:

а) загроза нелояльної поведінки персоналу за корисливими або особистими мотивами, що приводить до просочування критичної інформації або порушень режиму забезпечення загальної безпеки;

б) загрози порушення захисту від несанкціонованого доступу до корпоративної мережі унаслідок халатності або низького професійного рівня персоналу;

в) загрози проведення ними прямих диверсійних дій або саботажу з боку персоналу, схиленого до співпраці сторонними особами або організаціями;

г) загрози появи (застосування) в процесі звільнення (особливо унаслідок виникнення конфлікту) персоналу, що мав відношення до забезпечення загальної безпеки або захисту корпоративної мережі від несанкціонованого доступу, пристроїв або програм, що порушують режим забезпечення інформаційної безпеки;

д) загрози використання персоналом ресурсів корпоративної мережі і оброблюваної в ній інформації в особистих цілях;

е) загрози нелегального фізичного підключення додаткового робочого місця до кабельних ліній корпоративної мережі з метою отримання доступу до мережі і циркулюючої нею інформації.

Методи протидії зовнішнім і внутрішнім загрозам інформаційної безпеки. Відповідно до описаним видам загроз можливі наступні методи протидії ним:

- для видів 1а, 2в – забезпечення загального режиму безпеки на території і в приміщеннях підприємства (організації);

- для видів 1б, 1в, 1г, 2е – вживання комплексу програмно-технічних і спеціальних режимних заходів щодо захисту корпоративної мережі і циркулюючої в ній інформації, за результатами – проведення організаційно-штатних заходів;

- для видів 1д, 2а, 2б – проведення необхідних організаційно-штатних заходів, для виду 2б додатково - проведення роз'яснювальної і профілактичної роботи;

- для видів 2г, 2д - координоване проведення спеціальних режимних і технічних заходів.

Таким чином, для вирішення проблеми в комплексі необхідно планувати проведення програмно-технічних заходів щодо захисту мережі і циркулюючої по ній інформації від несанкціонованого доступу, закупівлю відповідного програмного і апаратного забезпечення, розробити заходи щодо забезпечення загального режиму безпеки, а також спеціальні заходи щодо забезпечення особливого режиму використання критичної інформації і доступу до неї.

Організаційно-технічні заходи щодо забезпечення режиму інформаційної безпеки. Для забезпечення режиму інформаційної безпеки в рамках органу внутрішніх справ доцільно вжити наступні заходи:

- узяти під жорсткий контроль всі канали зв'язку, по яких корпоративна мережа може сполучатися із зовнішнім світом (телефонні комутовані, виділені, цифрові, радіоканали тощо);

- організувати розмежування доступу в мережі до різних інформаційних ресурсів шляхом розбиття мережі на ізольовані сегменти, для кожної групи користувачів мережі надати строго тільки необхідні ресурси;

- виділити експлуатований *WWW*-сервер в окремий ізольований сегмент, а при необхідності і фізично ізолювати його від решти мережі;

- видалити (заблокувати) на експлуатованих в мережі комп'ютерах накопичувачі на змінних носіях, видалити або опечатати шлейфи невживаних комунікаційних портів, для інших встановити нестандартні зовнішні роз'єми, експлуатація яких без спеціального ключа (перехідника) неможлива, при нагоді використовувати як робочі місця термінали замість персональних комп'ютерів;

- ключі для комунікаційних портів зберігати в опечатаних пеналах в металевому сховищі і видавати строго певним співробітникам;

- перенесення будь-якої інформації з комп'ютера на комп'ютер крім мережі здійснювати тільки на одному зовнішньому накопичувачі, при цьому займатися цим повинен один конкретний співробітник, який має нести персональну відповідальність за збереження інформації;

- носії, на яких фізично розміщується критично важлива інформація, помістити в контейнери типу *Mobil rack*, опечатувати замки і передню панель контейнера при експлуатації масиву, в неробочий час поміщати контейнер в металеве сховище (сейф);

- офіційно призначити співробітника, який несе відповідальність за захист інформації на підприємстві (в організації), визначити коло його обов'язків (За законом відповідальність за захист інформації несе керівник органу. Він може призначити наказом відповідального або службу захисту інформації);

- провести суцільну перевірку комп'ютерів, що експлуатуються на підприємстві (в організації) на предмет нештатних закладок або підключень, після перевірки корпуси комп'ютерів опечатати;

- для припинення спроб зняття інформації з працюючих комп'ютерів шляхом візуального спостереження або сканування електромагнітної сигнатури обладнати вікна в приміщеннях, в яких розміщуються комп'ютери, внутрішніми жорсткими металевими жалюзі, зобов'язати персонал закривати жалюзі при обробці критичної інформації;

- для збереження найкритичнішої інформації як зберігається на носіях, так і переміщається по мережі, застосовувати криптографічне програмне забезпечення, що використовує сучасні алгоритми шифрування;

- постійно сканувати простір корпоративної мережі і поступаючи ззовні інформацію антивірусними програмами, регулярно обновляти бази даних антивірусів, зобов'язати персонал систематично перевіряти носії, особливо змінні, а також вхідну пошту, на предмет наявності вірусів;

- встановити дисциплінарну відповідальність персоналу за порушення режиму інформаційної безпеки і недбале відношення до збереження інформації, кожний випадок порушення режиму і вжиті відносно порушника дисциплінарні заходи доводити до зведення колективу, акцентувати увагу персоналу на тому, що розповсюдження шкідливих програм (вірусів) і порушення правил

експлуатації комп'ютерів і їх мереж, що призвело втрату (пошкодження) інформації, в даний час є кримінально караними діяннями;

- встановити штатно передбачені паролі на доступ до *BIOS* комп'ютерів, на комп'ютерах, які містять критичну інформацію додатково встановити паролі на завантаження, передбачити систему парольної ідентифікації користувачів в мережі, ведення протоколів роботи користувачів;

- встановити в корпоративній мережі внутрішні *POP*, *SMTP*, *Proxy HTTP*/*FTP* серверу, все спілкування користувачів мережі із зовнішнім світом здійснювати тільки через ці серверу, встановити на них програмне забезпечення для об'єктивного контролю за вмістом інформації, яка циркулює через них;

- встановити на комп'ютерах, у тому числі і не підключених до мережі, засобів об'єктивного контролю за діяльність персоналу;

- встановити програмну систему моніторингу руху пакетів в корпоративній мережі і доступу до критичної інформації, вести протоколювання доступу до подібної інформації;

- встановити програмну систему типу *packet sniffer* для сканування мережі, при виникненні ризику порушення режиму безпеки переводити її в режим перехоплення пакетів;

- призначити конкретного співробітника, який займатиметься аналізом результатів роботи засобів об'єктивного контролю, контролювати стан безпеки мережі і при виникненні нештатних ситуацій вживати заходи по негайному реагуванню;

- систематично перевіряти дотримання режиму інформаційної безпеки - збереження печаток на устаткуванні, ключів комунікаційних портів, зовнішніх і змінних носіїв, носіїв у контейнерах, наявність нетабельних комунікаційних пристроїв і носіїв на робочих місцях персоналу, наявність комп'ютерів, залишених персоналом у включеному стані без нагляду.

Короткі рекомендації з організації розмежованого доступу в мережі для невеликої організації. Початкові дані: є локальна мережа, яка об'єднує декілька відділів (або інших структурних підрозділів), Web-сервер і доступ до Інтернет.

Потрібен: розмежувати права доступу на рівні відділів/підрозділів до ресурсів інших підрозділів і забезпечення безпеки при роботі з Інтернетом в плані несанкціонованого доступу з Інтернету до внутрішньої мережі організації.

Пропонується наступне рішення: мережа організації розбивається на сегменти за допомогою збору сегментів мережі на РІЗНИХ концентраторах (хабах). Усередині одного сегменту передбачається, що всі машини мають однаковий рівень доступу. В центрі мережі ставиться машина під ОС Linux з набудованими правилами фільтрації. Для кожного сегменту в сервері передбачається окрема мережна платня.

Доступ з одного сегменту в інший може бути дозволений або заборонений повністю або частково. Під частковим обмеженням доступу слід розуміти наступні види обмежень:

1. По *IP*-адресі джерела і приймача пакету.

2. По протоколу *TCP*/*UDP*/*ICMP*.
3. По порту джерела і приймача пакету.
4. По ознаці *SYN*/*ACK* (ініціатор/відповідач).
5. По інтерфейсах головного маршрутизатора.

Крім того, може бути виконана жорстка прив'язка *IP*-адрес до *MAC*- адрес мережної плати на робочих машинах при їх роботі з/через головний маршрутизатор, що утрудняє просту перестановку *IP* адреси навіть усередині одного сегменту з машини на машину для запобігання представленню однієї машини реквізитами іншої в мережі. (Правда при цьому не виключається перестановка мережної плати фізично з машини на машину або, за наявності у мережній платі такої можливості, перепрограмування її *MAC*-адреси на апаратному рівні. Проте ці дії вимагають високої кваліфікації користувача, легко виявляються при дубляжі MAC-адрес у вигляді порушення роботи двох робочих машин у мережі).

Приклад схеми приведений на рис. 6.6.

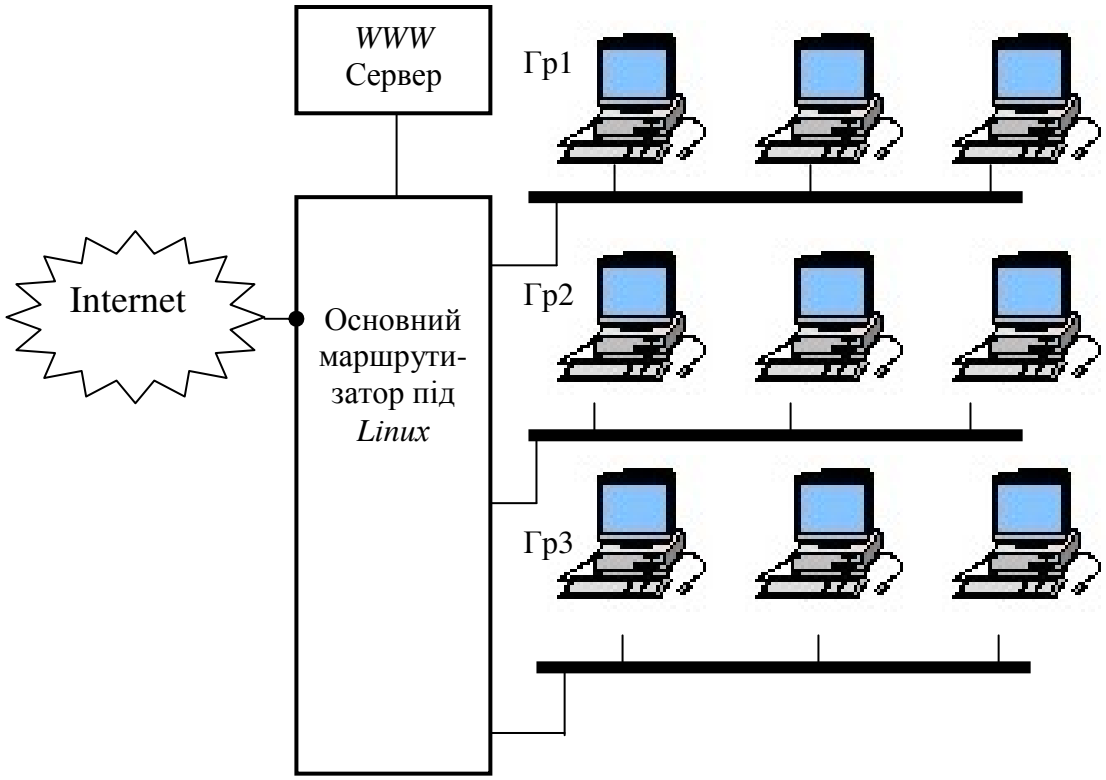

Рисунок 6.6 – Приклад сегментації мережі

На рис. 6.6 показано 3 підмережі для організації 3 роздільних сегментів, внутрішній трафік яких не може прослуховуватися в режимі сніффування з іншого сегменту мережі. *WWW*-сервер у вказаному прикладі винесений в окремий сегмент на окрему машину. Це виправдано, якщо потрібна велика закритість і надійність машини під *Linux*. Хоча у багатьох випадках *WWW* сервер може бути розміщений прямо на *Linux*-машині. Доступ при цьому до даного *WWW* серверу може бути розмежовано за описаних вище умов

незалежно від того на окремій машині або на машині-маршрутизаторі знаходиться *WWW*.

Адміністрування власне *Linux* і *WWW* серверів може проводитися з самого серверу або з будь-якої з робочих станцій. Доступ для адміністрування може бути додатково захищено від прослуховування трафіку усередині свого сегменту.

Всі вище перелічені обмеження застосовні і до виходу через даний *Linux*-сервер в Інтернет і для блокування несанкціонованого проникнення з інтернету у внутрішні сегменти. Крім того на даному *Linux*-сервері можуть бути встановлені *proxy*-сервери для доступу до Інтернету, у тому числі і з можливістю фільтрації запрошуваних доменних імен при серфінгу по Інтернету для блокування відвідування небажаних сайтів.

Крім того, може бути на базі *Linux* організовано поштовий сервер *SMTP*/*POP*3 і модемні підключення для доступу ззовні.

Всі описані рішення практично незалежні і можуть додаватися поступово за мірою необхідності.

Умовний кошторис проведення робіт по забезпеченню режиму інформаційної безпеки. Технічні засоби і заходи:

- придбання контейнерів типа *Mobil rack* 2-3 шт. по 10-15 УЗЕ;
- виготовлення нестандартних роз'ємів зовнішніх інтерфейсів (*LPT*) і ключів до них 7-9 УЗЕ за комплект;
- придбання комп'ютера-маршрутизатора і мережних апаратних засобів до нього 700-1000 УЗЕ;
- придбання зовнішнього накопичувача з інтерфейсом *LPT* 140-175 УЗЕ
- відключення накопичувачів на змінних носіях, зовнішніх інтерфейсних роз'ємів за потребою;
- виготовлення і установка приладдя для опечатання корпусів комп'ютерів, контейнерів з вінчестерами, виготовлення (закупівля) пеналів для зберігання ключів роз'ємів LPT за потребою;
- установка на вікнах в приміщеннях з комп'ютерами захисних жалюзі за потребою;
- органолептичний контроль наявності сторонніх закладок на робочих станціях мережі 2-4 УЗЕ на робоче місце.

Програмні засоби:

- установка і конфігурація програмного забезпечення маршрутизатора і брандмауера 200 УЗЕ;
- розробка, установка, конфігурація засобів об'єктивного контролю робочих місць мережі 4 УЗЕ на робоче місце;
- установка і конфігурація POP/SMTP і HTTP серверів і засобів об'єктивного контролю на них 100 УЗЕ;
- конфігурація системи розмежування доступу користувачів 50 УЗЕ;
- установка і конфігурація системи типу *packet sniffer* для роботи в режимі сканування мережі 150 УЗЕ;

- установка системи моніторингу руху пакетів в корпоративній мережі і доступу до критичної інформації 60 УЗЕ;
- придбання антивіруса AVP з річною підпискою 100 УЗЕ
- придбання антивіруса DoctorWEB за потребою
- установка і конфігурація засобів шифрування даних за потребою.

Далі перейдемо до розгляду процедур проектування системи інформаційної безпеки центрів обробки викликів та контакт- центрів.

6.7 Комплексна система інформаційної безпеки центрів обробки викликів

Модель безпеки центра обробки викликів. Мета захисту ЦОВ полягає у виконанні норм, заходів та дій, спрямованих на запобігання шкоди і/або збитків у разі реалізації загрози чи у разі атаки на інформаційну безпеку. Захист здійснюється комплексною системою захисту (КСЗ) ЦОВ, яка складається з правового, організаційно-методичного, технічного, програмного, інформаційного та математичного забезпечень, що запобігають або суттєво утруднюють завдання шкоди функціонуванню ЦОВ.

Політика безпеки ЦОВ або стандартний функціональний профіль захищеності оброблюваної інформації [28] повинні визначатись відповідно до чинної нормативно-правової бази та відповідати категоріям за ознакою режиму доступу інформації, яка обробляється у ЦОВ. У ЦОВ обробляється: інформація споживачів і множина даних телекомунікаційних та інформаційних послуг; технологічна інформація та інформація, необхідна для керування ЦОВ; інформація, необхідна для захисту ЦОВ. Підрозділи оператора зв'язку отримують та обробляють сотні й тисячі звернень клієнтів, генерують великий обсяг службової інформації.

Головним об'єктом загроз у ЦОВ є телекомунікаційні й інформаційні послуги, інформація споживачів, технологічна інформація КСЗ та технологічна інформація щодо адміністрування та керування обчислювальною системою ЦОВ і засобами обробки інформації – дані про мережні адреси, імена, персональні ідентифікатори та паролі користувачів (тут і далі користувачі – це персонал ЦОВ, на відміну від споживачів послуг ЦОВ), їхні повноваження та права доступу до об'єктів, інформація журналів реєстрації дій користувачів, інша інформація баз даних захисту, встановлені робочі параметри окремих механізмів або засобів захисту, інформація про профілі обладнання та режими його функціонування, робочі параметри функціонального ПЗ тощо. Технологічна інформація призначена для використання тільки уповноваженими користувачами: співробітниками служби безпеки ЦОВ та персоналом, що забезпечує його функціонування.

КСЗ має забезпечувати реалізацію вимог із захисту цілісності та доступності загальнодоступної інформації, що, циркулює в ЦОВ, телекомунікаційних та інформаційних послуг. Одночасно, має забезпечуватись конфіденційність та цілісність технологічної інформації, інформації керування та захисту ЦОВ. Забезпечення цілісності інформації полягає у забезпеченні її повноти, точності та достовірності. Забезпечення доступності полягає у наданні доступу до

інформації за наявності відповідних повноважень. Забезпечення конфіденційності полягає у запобіганні несанкціонованому розпорядженню та використанню інформаційних ресурсів ЦОВ.

Технологія оброблення інформації має відповідати вимогам політики безпеки інформації, визначеної для ЦОВ. Вимоги щодо забезпечення цілісності загальнодоступної інформації ЦОВ та конфіденційності й цілісності технологічної інформації вимагають застосування технологій, що забезпечують реалізацію контрольованого і санкціонованого доступу до інформації та заборону неконтрольованої й несанкціонованої її модифікації. Технологія оброблення інформації має бути здатною реалізовувати можливість виявлення спроб несанкціонованого доступу до інформації ЦОВ та процесів, які з цією інформацією пов'язані, а також забезпечити реєстрацію в системному журналі визначених політикою відповідної послуги безпеки подій – як НСД, так і авторизованих звернень. Технологічними процесами має бути реалізована можливість створення резервних копій інформації *WEB*-сторінки та процедури їх відновлення з використанням резервних копій. Технологія оброблення інформації має передбачати можливість аналізу використання користувачами і процесами обчислювальних ресурсів автоматизованої системи і забезпечувати керування ресурсами.

Технічне, програмне, інформаційне забезпечення комплексної системи захисту ЦОВ повинні вирішувати дві основні задачі технічного захисту інформації ЦОВ: захист фізичного середовища ЦОВ; захист обчислювальної мережі ЦОВ. Загроза безпеці обчислювальної мережі ЦОВ визначається як потенційна можливість порушення безпеки функціональних та інформаційних об'єктів та ресурсів ЦОВ. Джерела загроз безпеці ЦОВ є: споживачі послуг ЦОВ; адміністратори ЦОВ; сторонні особи; спряжена телефонна мережа загального користування; програмні та технічні засоби, які реалізують функціональні об'єкти ЦОВ; техногенні аварії; стихійні лиха. Програмно-апаратні засоби захисту, що входять до складу КСЗ ЦОВ, повинні мати належним чином оформлені документи – експертні висновки, сертифікати, які засвідчують відповідність цих засобів вимогам нормативних документів системи ТЗІ.

З урахуванням типових характеристик середовищ функціонування та особливостей технологічних процесів оброблення інформації мінімально необхідний функціональний профіль можна вибрати по аналогії з нормативним документом [29]: КА-2, ЦА-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1. Функціональний профіль захисту обирається відповідно до вимог рівня захищеності інформації.

Організаційно-методичні заходи та норми в ЦОВ мають забезпечити проведення визначеної в ЦОВ політики безпеки. Проведення політики безпеки полягає у безперервності процесу оцінювання ризику від реалізації загроз ЦОВ та мінімізації можливої або заподіяної шкоди з прийнятним рівнем витрат.

Інфраструктура ЦОВ складає окремий від телекомунікаційної мережі – домен безпеки, де під доменом безпеки розуміються об'єкти та учасники, що є суб'єктами однієї політики безпеки і однієї адміністрації безпеки. До рівня

безпеки ЦОВ ставляться більш високі вимоги, ніж до цифрових телекомунікаційних мереж.

Характерними загрозами для ЦОВ є: перехоплення, ознайомлення зі змістом несанкціонованим споживачем і/або користувачем локально або віддалено; вилучення інформації, послуги або її частини, внесення невиявлених перекручень; маскараду – намагання особи відіграти роль іншої особи, приміром, при платних послугах; порушення зв'язку, недопущення взаємодії з ЦОВ або затримка інформації послуги; відмова від функціонування, випадкове або зловмисне використання об'єкта в нештатних режимах, повторний розиграш. Крім того, телекомунікаційне середовище оператора зв'язку підтримується популярними, але часто слабо захищеними, протоколами та інтерфейсами взаємодії – *TCP*/*IP*, *FTAM*, *CMIP*, *SNMP*, *FTP*, *HTTP*, *SMTP*, *X*25, *RS*232 тощо.

З боку телефонної мережі загального користування та мереж інших операторів загрозами (групами загроз) для ЦОВ можуть бути такі [30]:

маскування під логічний об'єкт;

спотворення або модифікація даних (споживача, користувача, з оплати, маршрутизації);

перехоплення даних, приміром для отримання інформації споживача;

відмова оператора зв'язку від того, що функціональний об'єкт передав чи отримав дані щодо оплати або іншу інформацію;

маскування, при якому зловмисник отримує несанкціонований доступ до послуг, а його рахунки сплачує інший споживач;

відмова у наданні послуги;

відмова абонента від з'єднання та інших виконаних ним дій;

неправильні дані з оплати; неправильні дані щодо взаєморозрахунків тощо.

Крім того, групу загроз обумовлюють невиконання вимог до безпеки проведення оперативно-розшукових заходів (закон України "Про телекомунікації", стаття 39, п. 4) та моніторингу телекомунікацій. Для всіх дій моніторингу мають бути забезпечені конфіденційність, цілісність та готовність [31]. При цьому, конфіденційність передбачає не тільки захист від розкриття зашифрованої інформації, але й приховання факту моніторингу. Всі функціональні об'єкти та інтерфейси, що відносяться до моніторингу, мають бути захищені від несанкціонованого доступу, розкриття та модифікації даних, що зберігаються та передаються.

Наслідками впливу загроз можуть бути: збитки внаслідок шахрайства, відтік клієнтів внаслідок втрати довіри до служби з боку споживачів, втрати внаслідок порушення персональних даних, втрати конфіденційності, штрафи за порушення законів, втрати споживачів у оплаті тощо.

Модель захисту інформаційних ресурсів ЦОВ розробляється на стадії технічного проектування. Вибір моделі захисту являє собою рішення задачі з мінімізації ресурсів захисту при забезпеченні наведеного в технічному завданні рівня захищеності інформаційних ресурсів ЦОВ. У результаті рішення визначається сукупність функціональних послуг захисту (ФПЗ) для реалізації КСЗ ТЗІ.

Матеріальну основу КСЗ ЦОВ повинна становити комп'ютерна база захисту, яку складають програмні та технічні засоби захисту, а також елементи функціональних об'єктів, які необхідно контролювати та якими необхідно керувати для реалізації політики безпеки.

Функції захисту інформації, що обробляється в ЦОВ. Послуги захисту та механізми, що їх реалізують, поділяються на штатні і додаткові (позаштатні). У сукупності зі штатними додаткові механізми повинні забезпечити зазначений у технічному завданні рівень захищеності інформації. На етапі проектування виконується оцінка реалізованих у ЦОВ штатних ФПЗ на відповідність наведеній у технічному проекті моделі захисту. Відсутні послуги реалізуються за допомогою додаткових засобів і механізмів захисту. Додаткові засоби розробляються, якщо рівень захищеності та рівень гарантій захищеності недостатній.

ЦОВ повинна реалізовувати такі функції захисту інформації.

1) Загальні послуги безпеки, які мають надаватись незалежно від складу і функціональних можливостей ЦОВ, а також під час інсталяції, обслуговування та керування програмними застосуваннями. Ці послуги потрібні у взаємодіях: користувачів із споживачами та між собою; користувачів з програмними застосуваннями; програмних застосувань між собою; програмних застосувань з ресурсами.

2) Спеціальні послуги безпеки, характерні для ЦОВ.

3) Додаткові, що розробляються й здійснюються при створенні ЦОВ для досягнення заданого рівня захищеності та гарантій.

КСЗ повинна надавати послуги для захисту: інформації користувачів та даних інформаційно-телекомунікаційних послуг; даних ЦОВ, у тому числі інформаційної бази керування; ресурсів ЦОВ; програмних засобів, телекомунікаційних засобів; технічних засобів; носіїв даних, у тому числі таких, що можуть переміщуватися. До складу загальних послуг безпеки ЦОВ мають входити: послуги ідентифікації та аутентифікації; послуга керування доступом, що повинна специфікувати множину припустимих для кожного суб'єкта операцій з кожним об'єктом і постійний контроль додержання цих специфікацій; послуга цілісності, що має забезпечити повноту, точність та достовірність інформації; послуга конфіденційності, що має забезпечити недоступність та нерозкриття інформації ЦОВ користувачам, що не мають для цього необхідних повноважень; послугу доступності.

Послуги безпеки ЦОВ реалізуються за допомогою загальних та спеціальних механізмів безпеки. Рівень захисту, визначений політикою безпеки ЦОВ, досягається вибором механізму безпеки відповідного класу. Ці класи, що можуть перетинатись, мають забезпечувати: запобігання атакам, виявлення атак, відновлення після атак. Для побудови КСЗ та керування безпекою ЦОВ, відповідно до стандартного функціонального профілю, використовуються такі загальні механізми безпеки:

за критерієм доступності: ДВ-1 - ручне відновлювання після збоїв, ДР-1 - квоти;

за критерієм конфіденційності: КА-2 - базова адміністративна конфіденційність;

за критерієм спостережності: НИ-2 – одиночне ідентифікування та аутентифікування; НК-1 - односпрямований вірогідний канал; НО-1 – розподіл обов'язків; НР-2 – захищений журнал; НТ-1 - самотестування за запитом; НЦ-1 – комплекс засобів захисту з контролем цілісності;

за критерієм цілісності: ЦА-1 – мінімальна адміністративна цілісність; ЦО-1 – обмежений відкат.

Для реалізації деяких послуг можуть використовуватись спеціальні механізми безпеки: цифровий підпис, нотаризація.

На практиці в основу інформаційної безпеки закладають стандартні сертифіковані рішення, що використовуються у сучасних серверних та клієнтських операційних системах з однократною реєстрацією користувачів. Для кожного користувача створюється профіль, відповідно до якого визначаються його права й можливості доступу до інформаційних ресурсів. Забезпечується ведення журналів й протоколювання усіх сеансів доступу користувачів до бази даних. У журналах фіксується вся інформація щодо дій, які виконуються у базі даних.

Вирішення задач забезпечення надійності, доступності і безперебійної роботи здійснюється у двох напрямах: забезпечення цілісності даних та програмних засобів; безперебійної роботи апаратних засобів. Забезпечення надійності апаратних засобів досягається застосуванням технології RAID, кластерної технології, резервним копіюванням програм та даних, безперебійним живленням серверного та мережного обладнання, застосуванням процедур перевірки цілісності та коректності даних. Для забезпечення надійного зберігання і передачі даних використовують технології створення резервних копій програм та даних і технології, що забезпечують гарантоване зберігання даних.

Запитання для самоконтролю

1. Дайте визначення, що є центром обробки викликів (ЦОВ) та його призначення.
2. Поясніть функції центру обробки викликів.
3. Як у стандарті визначається поняття «оператор»?
4. Поясніть структуру та принципи функціонування ЦОВ.
5. Поясніть призначення основних взаємодіючих програмно-апаратних функціональних одиниць ЦОВ.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ITU	–	(International Telecommunication Union) Міжнародний союз електрозв'язку
NGN	–	(Next Generation Networks) Мережі третього покоління
ТСО	–	(Total Cost of Ownership) Загальна вартість володіння
АС	–	Автоматизована система
АТС	–	Автоматична телефонна станція
ВВС	–	Взаємодія Відкритих Систем
ДССЗЗІ	–	Державна служба спеціального зв'язку та захисту інформації
ЕОМ	–	Електронно-обчислювальна машина
ЕОД	–	Електронний обмін даними
ЕЦП	–	Електронний цифровий підпис
ЗМІ	–	Засоби масової інформації
ІБ	–	Інформаційна безпека
ІР	–	Інформаційні ресурси
ІС	–	Інформаційна система
ІКТ	–	Інформаційно-комунікаційні технології
ІТ	–	Інформаційні технології
КЗМЗ	–	Комплекс засобів і механізмів захисту
КЗІ	–	Комплексний захист інформації
КСЗІ	–	Комплексна система захисту інформації
КСІБ	–	Комплексна система інформаційної безпеки
ЛОМ	–	Локальна обчислювальна мережа
МПД	–	Мережа передавання даних
МЗК	–	Мережі загального користування
МТЗ	–	Міський телефонний зв'язок
МТС	–	Матеріально-технічні засоби
МЦОВ	–	Центр обробки викликів служби «Міліція»
ОІД	–	Об'єкт інформаційної діяльності
ПЕМВН	–	Побічні електромагнітні випромінювання та наводок
РНБО	–	Рада національної безпеки та оборони
РСО	–	Режимно-секретний орган
СЗІ	–	Система захисту інформації
СЗН	–	Соціальний захист населення
СІБ	–	Система інформаційної безпеки
СЦЗІ	–	Соціальний захист інформації
ТЗІ	–	Технічний захист інформації
ТМЗК	–	Телекомунікаційні мережі загального користування
ТфМЗК	–	Телефонна мережа загального користування
ФВА	–	Функціонально-вартісний аналіз
ФЗП	–	Фонд заробітної плати
ФПЗ	–	Функціональні послуги захисту
ЦОВ	–	Центр обробки викликів
ЦСК	–	Цифрові системи комутації

ПЕРЕЛІК ПОСИЛАНЬ

1. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. – К.: Кондор, 2004. – 384 с.

2. Закон України „Про Національну програму інформатизації” від 04.02.1998 р. № 74/98-ВР. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=74%2F98%2D%E2%F0&p=1181903521686018

3. Рубан В.Я. Інформаційна безпека України: сутність та проблеми // Стратегічна панорама. – 1998. – № 3-4. – С. 170.

4. Організація і сучасні методи захисту інформації; За ред. С.А. Дієва та А.Г. Шаваєва – М., 1998. – 52 с.

5. Закон України „Про телекомунікації” від 18.11.03 р. № 1280-IV. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1280%2D15&p=1

6. Закон України „Про захист інформації в автоматизованих системах” від 5.06.1994 р. № 81/94-ВР. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=40966&cat_id=38828

7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. – С 12.

8. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40371&cat_id=38835

9. НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

10. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

11. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

12. НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. – Режим доступу:

http://www.dsszzi.gov.ua/dstszi/control/uk/publish/
article?art_id=40339&cat_id=38835

13. НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова).

14. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

15. КНД 45-164-2001. Типова модель загроз для формування ресурсів цифрових АТС, що використовуються в мережах електрозв'язку загального користування України. – Режим доступу: http://www.stc.gov.ua

16. ISO/IEC 15408:2000 Части 1 – 3. "Информационные технологии. Общие критерии оценки безопасности информационных технологий (ИТ – безопасности)", ISO/IEC 13335:1997 «Руководство по управлению ИТ – безопасностью», ИСО/МЭК 17799:2000 "Практические рекомендации по управлению ИТ-безопасностью".

17. НД ТЗІ 3.7-003-03. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

18. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

19. Домарев В.В. Математические модели систем и процессов защиты информации.Електронний ресурс http://www.domarev.kiev.ua/nauka/. С.56.

20. Кравченко В.П. Система поддержки принятия решений. Електронный ресурс: http://it2b.ru/it2b2.viev5.page21.html.

21. Черноруцкий И.Г. Методы оптимизации и принятия решений. С.-Пб, 2001, С. 248.

22. Организация планирование и управление предприятиями связи / Е.В. Демина, Е.К. Иодко, Л.И. Майофис, Н.П. Резникова. – М.: Радио и связь, 1990. – 352 с.

23. Котенко М. Центры обработки вызовов // Телеком № 9-10 (27-28)/2000. С.56-63.

24. Гольдштейн Б.С., Зарубин А.А., Потапов А.И. Центры обработки вызовов для органов внутренних дел: учебное пособие // СПбГУТ. – СПб. – 2005. – 52 с.

25. Петренко С. Методические основы защиты информационных активов компании // Режим доступу: – www.infosecurity.ru/ gazeta/content/031104/article03.html.

26. Шварц М. Сети ЭВМ. Анализ и проектирование / Пер. с англ. Под ред. В. А.Жожикашвили – М.: Радио и связь, 1981. – 336 с.

27. Корнышев Ю. Н., Мамонтова Н. П. Задачник по теории телефонных и телеграфных сообщений. – Одесса: ОЭИС, 1974. 139 с.

28. Корявцев П.М. Общий комплекс мер по обеспечению инфрмационной безопасности. Методические рекомендации // Вестник МВД РФ. – М.: 2000.

29. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/ dstszi/control/uk/publish/article?art_id=40381&cat_id=38835

30. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/ dstszi/control/uk/publish/article?art_id=40342&cat_id=38835

31. Бельфер Р. А. Классификация угроз информационной безопасности сетей связи ВСС России (ISDN, IN, UMTS) и методы их количественной оценки // “Электросвязь”, М: – 2002, № 7. – С.14 – 18.

ЗМІСТ С.

Навчальне видання

Кононович Володимир Григорович, Стайкуца Сергій Володимирович, Тардаскіна Тетяна Миколаївна, Шинкарчук Тетяна Миколаївна

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦИФРОВИХ ПРОГРАМНО КЕРОВАНИХ АТС

Навчальний посібник для курсового та дипломного проектування

Навчальний посібник для дипломного та курсового проектування

Редактор *Л.А. Кодрул*
Комп'ютерне верстання *Ж.А. Гардиман*

Здано до набору
Підписано до друку Обсяг ум. -друк. арк.
Формат Зам. № Наклад прим.
Видруковано на видавничому устаткуванні фірми RISO
в друкарні редакційно-видавничого центру ОНАЗ ім. О.С. Попова
Одеса, 65021, вул. Старопортофранківська, 61
Тел. (0482) 720-78-94