Міністерство освіти і науки, молоді та спорту України

Одеська національна академія зв'язку ім. О.С. Попова

Кафедра інформаційної безпеки та передачі даних

В. Г. Кононович, С.В. Стайкуца, Т. М. Лемеха, Ю.В. Копитін

ІНФОРМАЦІЙНА БЕЗПЕКА ЦИФРОВИХ ПРОГРАМНО-КЕРОВАНИХ АТС

Навчальний посібник
для курсового та дипломного проектування

Одеса 2013

Міністерство освіти і науки, молоді та спорту України

Одеська національна академія зв'язку ім. О.С. Попова

Кафедра інформаційної безпеки та передачі даних

В. Г. Кононович, С.В. Стайкуца, Т. М. Лемеха, Ю.В. Копитін

ІНФОРМАЦІЙНА БЕЗПЕКА 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 ред. члена-кореспондента МАЗ, кандидата технічних наук, доцента В.Г. Кононовича

Одеса 2013

ББК 004.056.5(075.8); 681.336; 342.4

План НМВ 2012 р.

Рецензенти:

Климаш М.М., д.т.н., професор, завідувач кафедри телекомунікацій, Національний університет «Львівська Політехніка»;

Кадацький А.Ф., д.т.н., професор, завідувач кафедри безпеки виробничих процесів та електроживлення систем зв'язку, Одеська національна академія зв'язку ім. О.С. Попова

Інформаційна безпека цифрових програмно-керованих АТС : [навч. посіб.] / **В.Г. Кононович , С.В. Стайкуца, Т.М. Лемеха, Ю.В. Копитін;** за ред. чл.-кор. МАЗ **В.Г. Кононовича**. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – С.

ISBN

Представлені основні положення, поняття й визначення з проектування систем технічного захисту інформації програмно-керованих автоматичних телефонних станцій, зокрема, органів державної влади, організаційного, правового, технічного, методичного та програмно-апаратного забезпечення на етапах створення, введення в дію та технічної експлуатації комплексних систем технічного захисту інформації. Викладаються методи техніко-економічного обґрунтування ефективності інформаційної безпеки.

Висвітлено методологію проектування захисту автоматизованих центрів оброблення викликів (call – centre) та надання державних послуг на прикладі центру оброблення викликів для органів внутрішніх справ (служби «102» – Міліція).

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

Для студентів старших курсів вищих навчальних закладів.

СХВАЛЕНО
кафедрою інформаційної безпеки та передачі даних.
Протокол № 5 від 07.04.2009 р.

ЗАТВЕРДЖЕНО
методичною радою академії зв'язку
Протокол № 16 від 23.03.2012 р.

ISBN

ВСТУП

Інформатизація, інтеграція, глобалізація та прискорений розвиток телекомунікацій чинять значний 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, спрямованої 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.

Актуальною 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 удосконалення системи інформаційної безпеки та процесу управління інформаційною безпекою.

Цей навчальний посібник повинен допомогти студентам, які навчаються за напрямами підготовки 1601, 1701 в галузі знань «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 передачі даних В.Г. Кононович (вступ, розд. 1 – 4); аспірант Ю.В. Копитін, (розд. 8); к.ф.н., доцент кафедри інформаційної безпеки та передачі даних С.В. Стайкуца (розд. 3, 5, 7); викладач кафедри інформаційної безпеки та передачі даних Т.М. Лемеха (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 низка 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, робить 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 отримання, 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, а саме:

– 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, отже, 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 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 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 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.

В роботі [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 уточнені 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 соціально-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 збитків 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 у систематичному аналізі і контролі можливості появи реальних або потенційних загроз і своєчасних заходів для їхнього попередження;

– на локалізацію злочинних дій і вживання заходів з 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 з 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 отримання 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, отримують електронно-обчислювальні машини (ЕОМ), в яких може відбуватися не тільки витік інформації, але й 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 й управління захищеною інформацією;

– запобігання витоку і втрати інформації;

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

– 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 отримання, 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 отримання). 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 та 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 оброблення викликів та центрів надавання послуг з автоматичним чи напівавтоматичним голосовим спілкуванням з клієнтами.

1.3 Постановка задач проектування

Метою проектування є виконання етапів та стадій створення комплексної системи інформаційної безпеки (КСІБ), об'єктів інформаційної діяльності (ОІД), телефонних комунікаційних систем (цифрових АТС, центрів оброблення 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 [7]:

– прийняття рішення щодо створення системи інформаційної безпеки;

– розробка Технічного завдання на проектування КСІБ;

– проектування КСІБ згідно з вимогами Технічного завдання та перед проектних досліджень;

– будівництво, випробування, атестація, державна експертиза та здавання КСІБ до експлуатації;

– технічна експлуатація та удосконалення 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 у 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 оброблення 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 й 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 зі своїм варіантом.

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

15. Скласти опис послуг і механізмів безпеки у 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 з обраним рівнем 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 периметра ІАС – міжмережних 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 оброблення викликів, центр надавання державних послуг, центр управління комунікаціями тощо.

Питання 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 щодо 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 з нормативним документом [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 щодо захисту інформації.

У цьому розділі розкриваються основні принципи й напрями 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 автоматизованому обробленні 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, втрати, 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 з нормативно-правовою базою *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 вузла 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 і 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 лініями, 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.

В якості міжстанційних з'єднувальних ліній можуть використовуватись цифрові канали *E*1 з магістральної мережі *SDH* або *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 недокументовані функції і не контролюються системою технічної експлуатації вузла комутації.

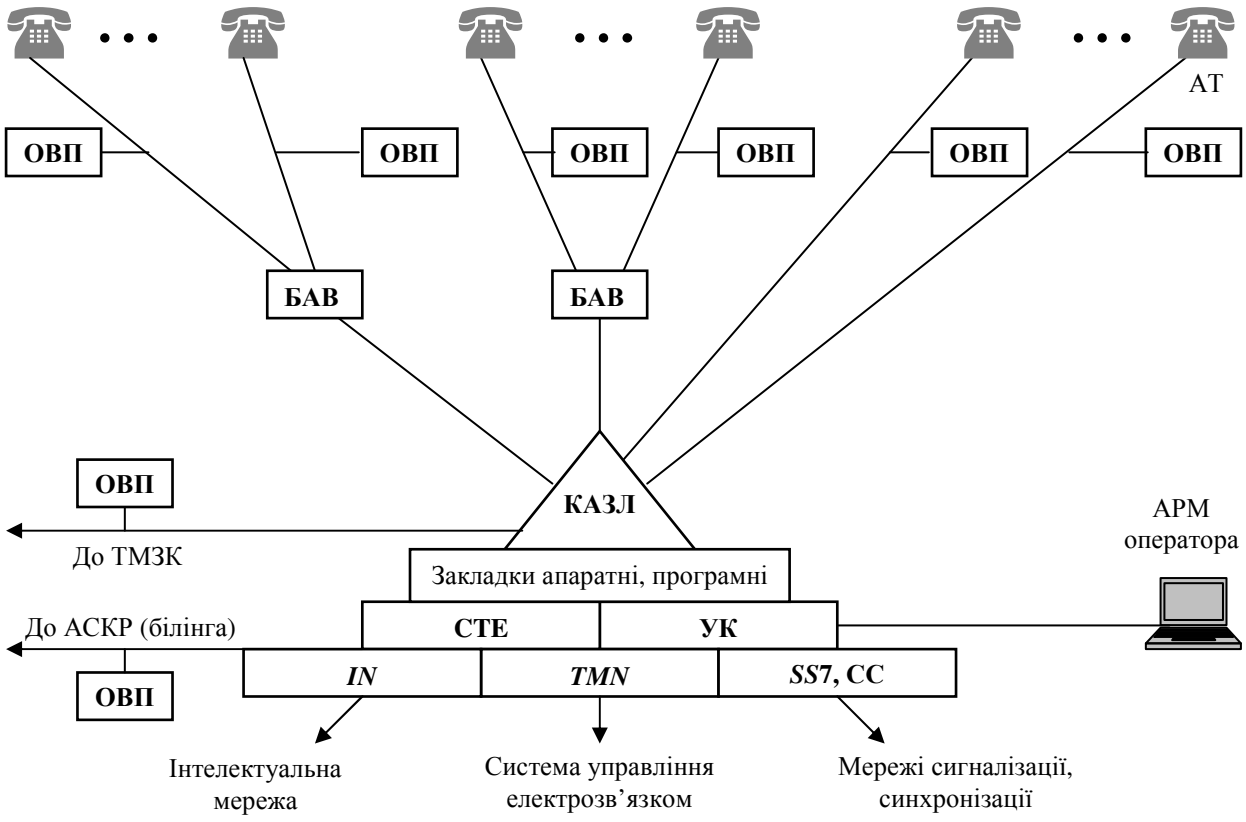

Рисунок 2.1 – Модель інфраструктури цифрового вузла комутації з позицій захисту інформації

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].

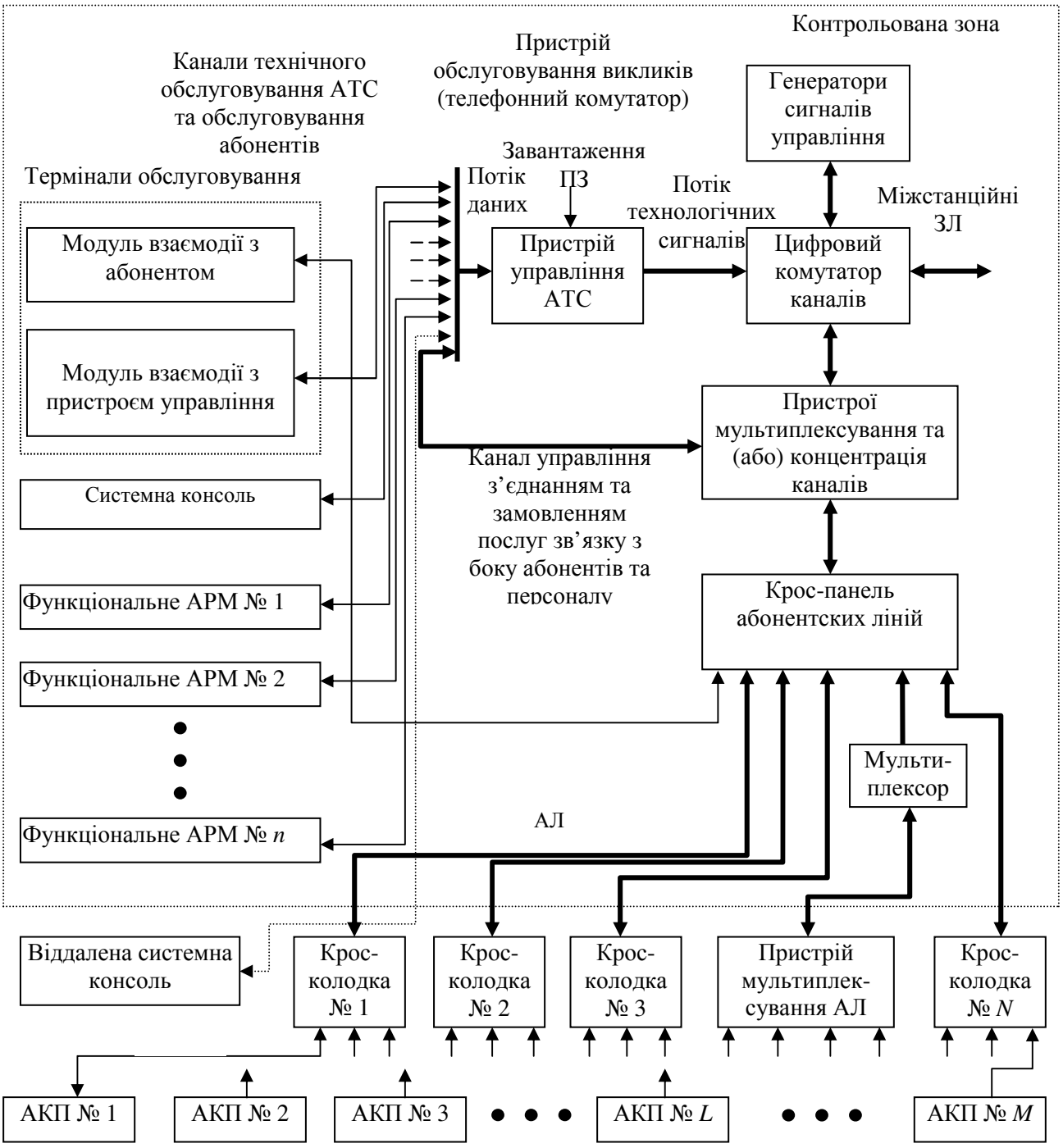

Рисунок 2.2 – Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ (з НД ТЗІ 1.1-001-99)

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 охоронному 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 з боку 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 обладнання 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 умови 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 з 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), проте 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.

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 значної 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 отримання 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 отримання 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 оброблення;

– утрата (ненавмисна втрата, витік) інформації та засобів її оброблення;

2) доступності:

– блокування інформації;

– знищення інформації та засобів її оброблення;

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 оброблення інформації;

– неякісні програмні засоби управління та оброблення 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, який надається їм штатними засобами. Виокремлено чотири рівні можливостей порушення НСД:

1 (найнижчий рівень можливостей) – запускання програм (задач) із фіксованого набору, який реалізує передбачені функції щодо оброблення інформації. Це обслуговуючий персонал, який 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 оброблення 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, які 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 оброблення інформації, які 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 білінга 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 каналах 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 обладнання 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 поділити 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 з боку віддаленого доступу у 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 напрямів. 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 спрямовані 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, за якого 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", яка 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, які 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, що реалізує несанкціонований вплив на ЦАТС;

– у *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 при 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 є 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 (в 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 виявлюваний НСД до інформації за допомогою спеціальних засобів доступу до аналогових і цифрових каналів, здійснювати виведення на запис, прослуховування або ретрансляцію несанкціоновано отриманих даних та мови. Захист в такому разі здійснюється плановим патрулюванням (пішим чи моторизованим) кабельних трас та посиленням контролю в періоди розв'язання важливих задач. Часто застосовують шифрування інформації.

Загрози інформації в цифрових системах передачі. Цифрові системи передачі мають вразливості на фізичному, канальному та мережному рівнях стека 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 передачі. Закладки можуть бути активізовані за допомогою радіоканалів. Після отримання 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 отримати 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 з Законом “Про телекомунікації” в ЦАТС та телекомунікаційних мережах, повинна бути забезпечена інформаційна безпека телекомунікаційних мереж, тобто здатність телекомунікаційних мереж забезпечувати захист від:

– знищення інформації;

– перекручування 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 факторів;

– 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 з Законами України “Про основи національної безпеки України”, “Про телекомунікації”, “Ліцензійних умов проводження діяльності у сфері телекомунікацій …” та іншими нормативно-правовими документами оператор у сфері діяльності з питань, пов’язаних з формуванням, використанням та захистом національних ресурсів має забезпечити інформаційну безпеку в таких напрямах:

– 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 автоматизованого оброблення 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 в експлуатацію, власне експлуатації, виведення з експлуатації та утилізації;

– на етапах узгодження засобів телекомунікацій, які можуть застосовуватися в телекомунікаційних мережах. Одними з критеріїв прийняття рішень є забезпечення надійності та безпеки мереж телекомунікацій. Розвиток та удосконалення 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 з нормами технологічного проектування та вимогами 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 з нормативними та технічними документами, чинними 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 з законодавством України.

Згідно з законодавством 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 державним інформаційним ресурсом, 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 з нормативними документами 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, втрати, 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 ускладнюють 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 елементах або "компенсаційним" методом, шляхом установлення відповідних засобів захисту в центрах та прикінцевому обладнанні.

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

Обладнання програмно-керувальних АТС та іншого обладнання ЦАТС має штатну систему захисту інформаційної безпеки, здатну забезпечувати захищеність рівня, який забезпечується фірмою-виробником даного обладнання згідно з договором 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 та 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 у 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 тою мірою, за якою 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 у 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 певні 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 дотримання 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 пророблені внаслідок ситуації з інформаційною безпекою, що склалася:

– зважаючи, що згідно з нормативно-правовими документами *передавання державних інформаційних ресурсів дозволяється лише через вузли комутації, що мають атестат відповідності КСЗІ вимогам із захисту інформації, який надається за результатами державної експертизи у сфері технічного захисту інформації,* пріоритетним є проведення робіт з розгортання 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 ступеня важливості інформації, розмірів імовірної 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 в усіх 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 у сфері ТЗІ, які для ЦАТС конкретизуються таким чином:

– розвиток й удосконалення системи ТЗІ;

– впровадження заходів щодо мінімізації можливості впливу загроз інформації, що передається, обробляється та зберігається в телекомунікаційних мережах;

– визначення механізму оцінки ступеня важливості інформації, розмірів імовірної 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 напрямів стандартизації у сфері ТЗІ й її пріоритетів; збирання, систематизація та аналіз відомостей щодо стану вітчизняної та зарубіжної нормативно-правової бази у 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 у 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;

– установлення 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 в інформаційну сферу ЦАТС;

– забезпечення конфіденційності інформації управління, тарифікації, персональних даних тощо; захист від порушення працездатності ЦАТС;

– розроблення нормативно-методичних документів з захисту інформації в мережі синхронізації вузлів зв'язку і мережі сигналізації SS 7.

Низка 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 у 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 реагуванні на швидкі зміни в ситуації.

Прогнозування та планування розвитку інформаційної безпеки в ЦАТС.

Планування заходів інформаційної безпеки з урахуванням напрямів 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.

Вирішення стратегічних питань зі створення підсистеми управління інформаційною безпекою ЦАТС.

Розроблення методики аналізу ризиків на основі якісних та кількісних оцінок ризиків.

Розроблення порядку та методик 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 введення 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 в 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, ступені гарантії безпеки інформаційного середовища ЦАТС, що базується на оцінках, за 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 у 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, установити 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, введення 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 поділити на первинні та основні. Основні засоби є обов'язковими, якщо КСЗІ ЦАТС планується атестувати на відповідність вимогам нормативних документів України у сфері ТЗІ. *Первинні* засоби впроваджуються на кожній ЦАТС. До їхнього складу входять:

– система захисту інформації автоматизованих робочих місць. Ця система має попереджувати НСД з робочих місць операторів. Рекомендується використовувати програмні чи апаратно-програмні комплекси захисту, які пройшли сертифікацію на відповідність вимогам по 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 з впровадження комплексу заходів й засобів захисту наступна:

– 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 центру управління інформаційною безпекою (центру реагування).

Впровадження системи безпеки ЦАТС і мережі може виконуватись поетапно, спочатку за "м'яким", а потім "жорстким" сценаріями. За "м'якого" сценарію будується захист мережі у точках спряження її з іншими мережами, вважаючи, що загрози мережі виходять ззовні, власні засоби є дружніми.

За "жорсткого" сценарію загроза може виходити з усіх напрямів, у тому числі і від внутрішніх елементів мережі. Захисна оболонка може бути прорвана й атака може бути переведена 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 під час 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, проектування та супроводження 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-керованому, 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 для 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 у сфері інформаційної безпеки.

Важливим є вироблення практичних підходів, прийомів, методики адекватної оцінки фактичної захищеності, засобів 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, пакета посадових інструкцій та дій в нештатних ситуаціях, обґрунтування необхідних вкладень у 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 наукоємних питань, а саме: 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 в

експлуатацію, власної 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 удосконалення 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, установленому 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 введення 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 з чинною нормативно-правовою базою ТЗІ для організації робіт зі створення КСЗІ у ЦАТС (чи для групи ЦАТС) створюється служба захисту інформації та призначаються відповідальні особи.

Організація та забезпечення діяльності у 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.

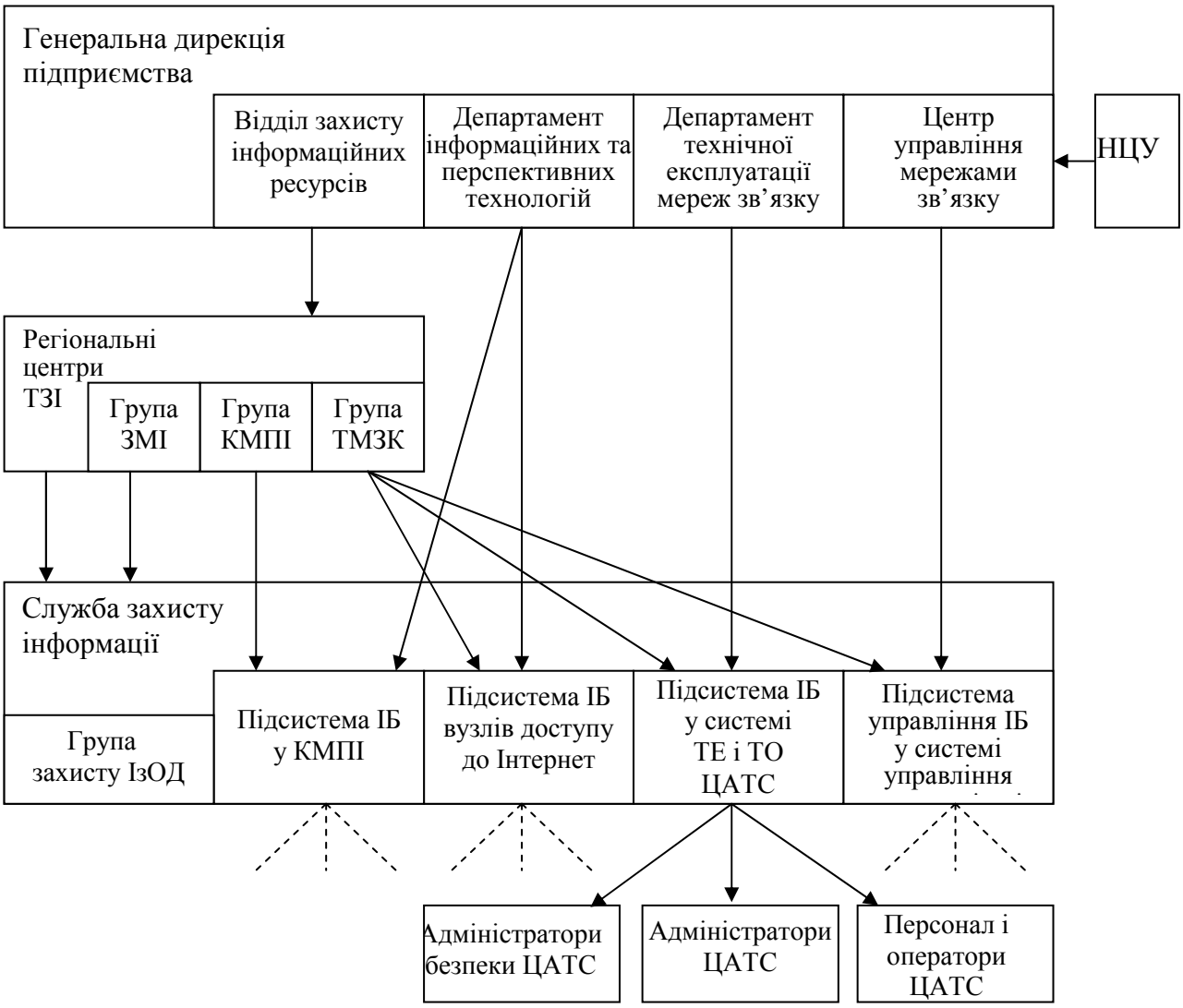

Рисунок 2.3 – Схема організації та забезпечення ТЗІ ЦАТС та мереж

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.

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 у складі існуючих.

У 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 терміни;

– створює і підтримує функціонування КСЗІ в ЦАТС у відповідності до державних і галузевих нормативних документів.

Група ТЗІ у складі Служби захисту інформації координує і контролює роботи щодо 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.

У ЦАТС обов'язки забезпечення інформаційної безпеки на робочих місцях покладаються на всіх, без винятку, працівників у межах означених в 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 з підтримання інформаційної безпеки на своїх робочих місцях і в закріпленому за ними обладнанні. Ці функції зазначаються у посадових інструкціях і в окремих інструкціях з інформаційної безпеки.

2.5.4 Організація управління інформаційною безпекою

Для безпосередньої організації роботи з забезпечення інформаційної безпеки (та/або захисту інформації) у структурі управління мережами телекомунікацій має бути створена служба управління інформаційною безпекою, яка повинна забезпечити виконання всього комплексу завдань захисту телекомунікаційних мереж та інформації. Цій службі підпорядковуються групи інформаційної безпеки, що створюються на ЦАТС (і/або у 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 експлуатація 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 доробки системи захисту з метою забезпечування її адекватності при зміні умов функціонування: характеристик системи, опрацьовуваної інформації, фізичного середовища, персоналу, призначення системи, політики безпеки тощо. Управління інформаційною безпекою базується на практичних правилах, які 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 порушення захисту чи інциденти у 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, що піддані ризику, а також зі збитками, що їх може бути нанесено підприємству через збої у системі захисту. Тому в процесі управління мають оцінюватись ризики порушення безпеки. Для оцінювання ризиків слід:

– визначати й аналізувати потенційні загрози, яким піддаються комп'ютерні системи, та їхні вразливості;

– розглядати збитки, які можуть нанести діяльності підприємства серйозне порушення інформаційної безпеки, з урахуванням можливих наслідків порушення конфіденційності, цілісності й доступності інформації;

– розглядати реальну ймовірність такого порушення 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:

– забезпечення безпеки має ґрунтуватися на виробничих цілях і вимогах;

– функції управління безпекою має взяти на себе керівництво підприємства;

– оцінювання ризиків порушення безпеки, загроз і слабкостей інформаційних ресурсів та рівня їхньої захищеності мають ґрунтуватися на цінності й важливості цих ресурсів;

– ознайомлення з системою безпеки всіх керівників та рядових співробітників підприємства;

– вивчання співробітниками політики та стандартів інформаційної безпеки;

– урахування 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 взаємоприєднаних 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 урахування 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” у підрозділах підприємства слід визначати згідно з НД ТЗІ 1.4-001-2000 [18].

Права й обов’язки адміністраторів безпеки визначаються наказом та інструкціями, затвердженими керівником підприємства.

Питання 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?
15. Які є головні завдання діяльності у сфері ТЗІ?
16. Поясніть головні напрями 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 введення 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 ЦАТС ТИПУ *EWSD*

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

3.1 Комплексна система 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.

3.1.1 Основні положення комплексної системи захисту інформації станції

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

Цифрові комутаційні системи (ЦКС), як правило, оснащуються штатними і, за необхідністю, 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. 3.1, де види забезпечення систем ТЗІ подані з різною глибиною деталізації. На рисунку є 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.

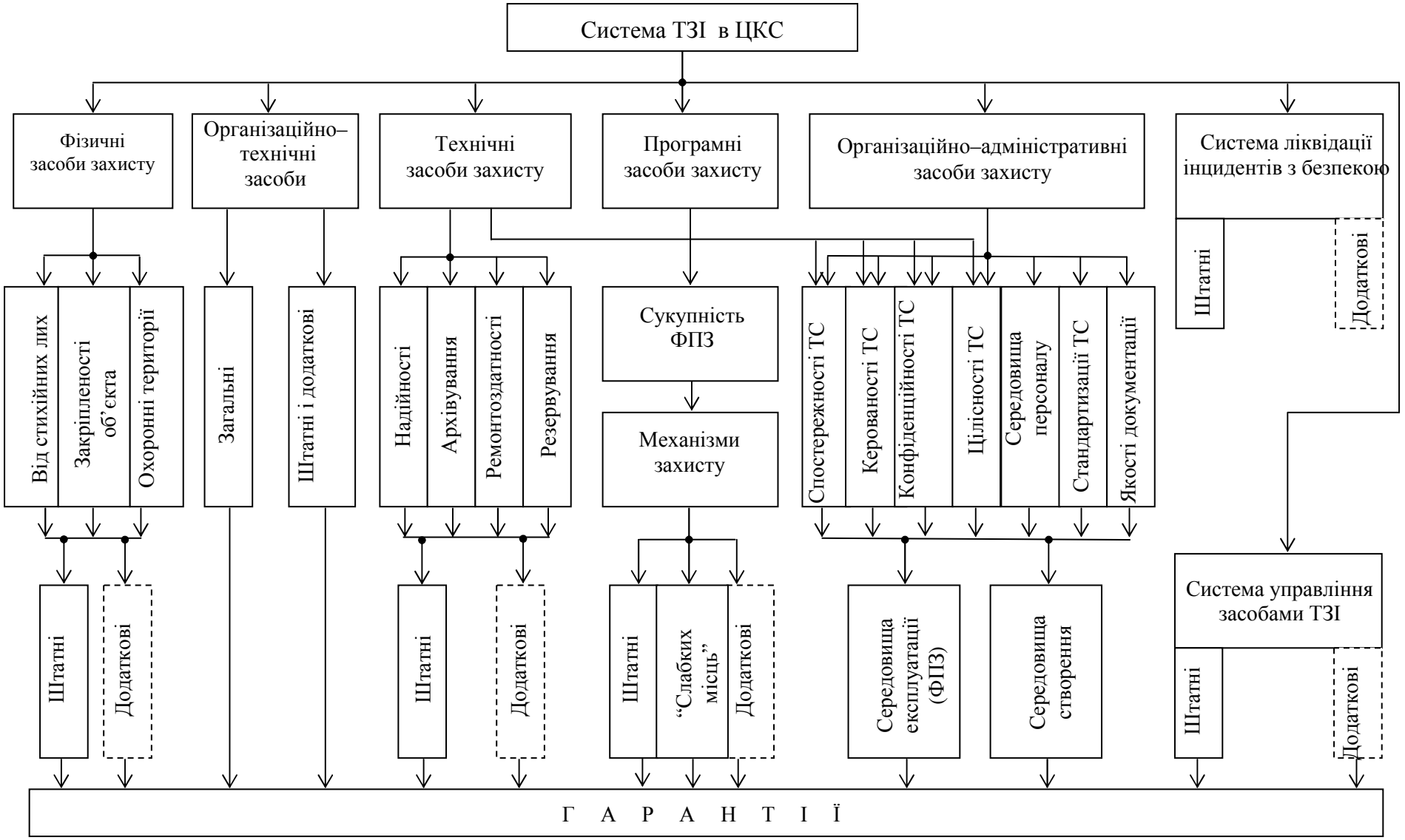

Рисунок 3.1 – Структура забезпечення системи ТЗІ в ЦКС

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 у 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 установлені в процесі її експлуатації; від впливів закладних пристроїв і програмних закладок;

– від впливів позаштатними технічними і/або програмно-технічними засобами на елементи обладнання в процесі експлуатації ЦКС; від витоків інформації через канали побічних електромагнітних витоків та наведень (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.

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 в 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 у 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 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. Вибір моделі захисту являє собою розв'язання задачі з мінімізації ресурсів захисту при забезпеченні наведеного в технічному завданні рівня захищеності інформаційних ресурсів ЦКС. У результаті розв'язання визначається сукупність ФПЗ для реалізації КЗМЗ у системі ТЗІ.

Для вперше створюваних ЦКС спочатку виконується вибір системи з оглядом 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 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.

3.1.2 Інформація, яка підлягає захисту

Для АТС з програмним управлінням (цифровим) під інформацією абонента розуміються розмови, а також поступово збільшувана частка високоякісних аудіо- та відеоповідомлень, 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 відносяться:

– 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.

– дані 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.

3.1.3 Загрози інформації

КСЗІ має протидіяти загрозам інформаційним ресурсам ЦАТС, до переліку 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 з 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.

3.1.4 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. 3.1. Читач може впевнитись, що наведений комплекс протистоїть усім видам загроз, наведеним у розд. 3.1.3.

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

Перший символ терма – літера Ф є заголовком терма.

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

Решта символів терма 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 літери);

– скорочення для позначення місць і (або) предметів розгляду (дві літери);

– скорочення для уточнення дій, місць та предметів розгляду (одна літера).

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

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

Ф – заголовок терма;

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. 3.1.

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

Таблиця 3.1 – 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
4. Несанкціонований доступ (НСД):	

Продовження табл 3.1

Специфікації ФПЗ	Найменування ФПЗ
1	2
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.	
1	2
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
4. 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)
5. 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 обладнання
6. НСД до модемної лінії доступу до модуля технічної експлуатації ЦКС EWSD	

Продовження табл 3.1

Специфікації ФПЗ	Найменування ФПЗ
1	2
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 абонентських каналів зв'язку ЦКС
1	2
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 обладнання
7. 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
8. 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 обладнання
Ф10/ПТД\М/РЕ\ЕУ	Наявність механічних засобів, що обмежують фізичний доступ до елементів устаткування ЦКС (нерозбірні зовні шафи, замкові пристрої і т. ін.)
9. Активізація пристроїв: 9.1. Активізація закладних пристроїв і (або) програмних закладок, що встановлені на (у) елементах підсистеми управління на передексплуатаційних стадіях життєвого циклу ЦКС EWSD; 9.2. 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 ускладнює можливість установлення закладних пристроїв (мінімальний вільний простір, компаунди, запаяні кожухи і т. ін.)
Ф10/ВКР/ПЗ/М	Використання модульності програмного забезпечення

Закінчення табл 3.1

Специфікації ФПЗ	Найменування ФПЗ
1	2
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.

3.1.5 "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. 3.2.

Таблиця 3.2 – «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

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

Злам у захисті – сертифікований канал можливої реалізації загроз для інформаційних ресурсів, механізми захисту для протидії яким 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 злами 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.

3.1.6. Загальні заходи захисту в комплексній системі захисту інформації в ЦКС типу EWSD

Комплексна система захисту інформації (КСЗІ) складається зі штатних (спеціальних) заходів і 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 тою мірою, якою 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, за 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.

3.2 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. 3.2. Управління станцією може здійснюватись безпосередньо з її території і віддалено з центру управління мережею. В 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 центру управління мережею та ЛОМ віддаленого управління мережею.

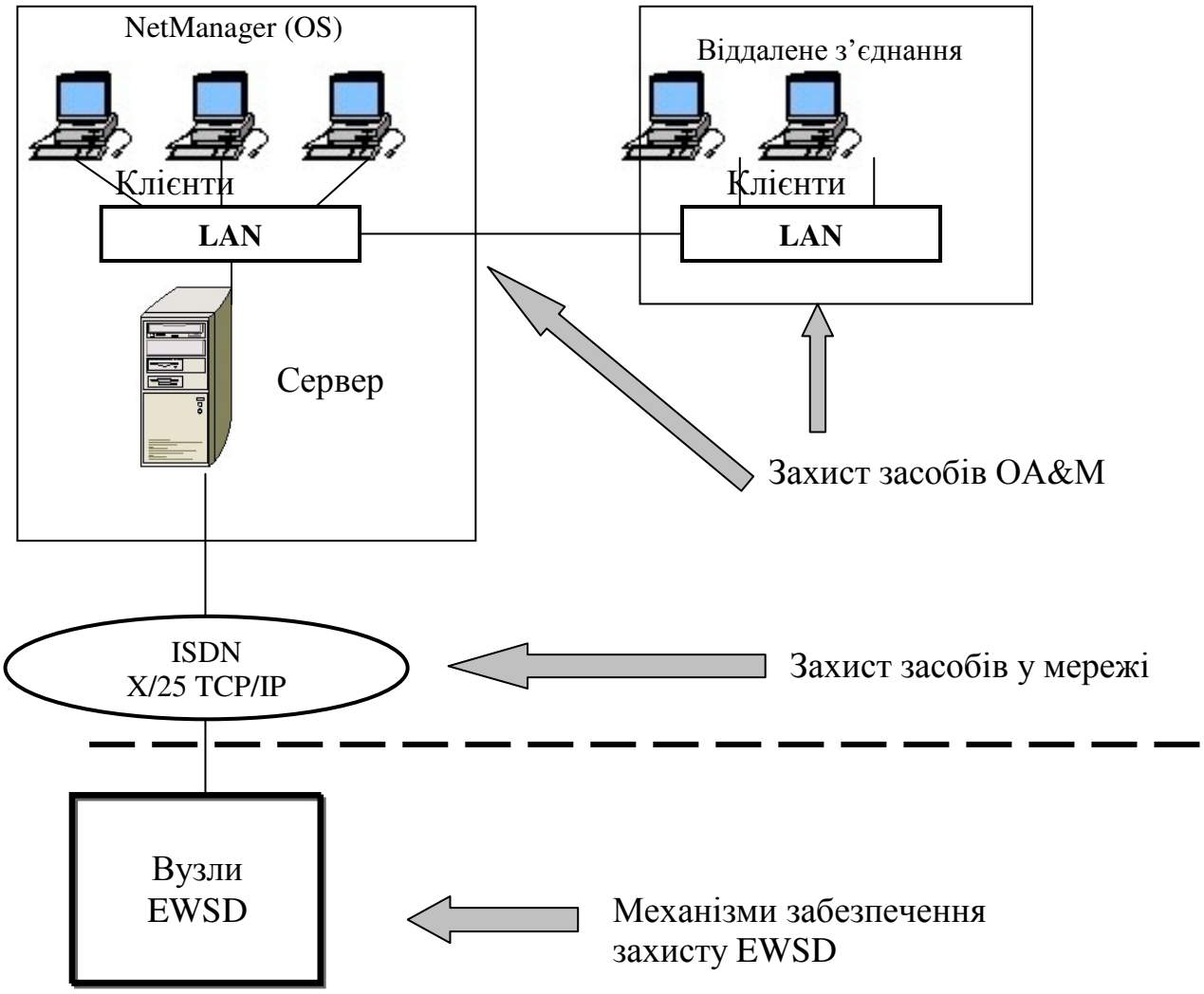

Рисунок 3.2 – Розподіл функцій захисту між вузлом *EWSD* і системою управління

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 будь-якої 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 трафіка від відправника до отримувача), 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 збирання статистики.

Інші скорочення та умовні позначення подані у розд. «Перелік умовних позначень та скорочень» 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 у системі управління станцією операційної системи *Windows NT*.

3.3 Функції та механізми забезпечення захисту в *EWSD*

Для розв'язання 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 передавання файлів.

3.3.1 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*:

1. 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*" домена *NT* є частиною локальної групи адміністраторів на всіх комп'ютерах *NetManager*. Усі користувачі *NetManager* призначаються групі "Користувачі *ENM*" ("*ENM Users*") домена *Windows NT*.

2. 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*).

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

4. 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 мережних вузлів *EWSD*, які їм були призначені адміністратором.

– механізми забезпечення захисту доступу для мережних вузлів *EWSD* відповідають аналогічним механізмам відповідної версії *EWSD*. Адміністратор призначає права користувача мережних вузлів 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 повторному використанню 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 у 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 надається індивідуальний ідентифікаційний код. Цей код повинен бути уведений 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 та 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. 3.3.

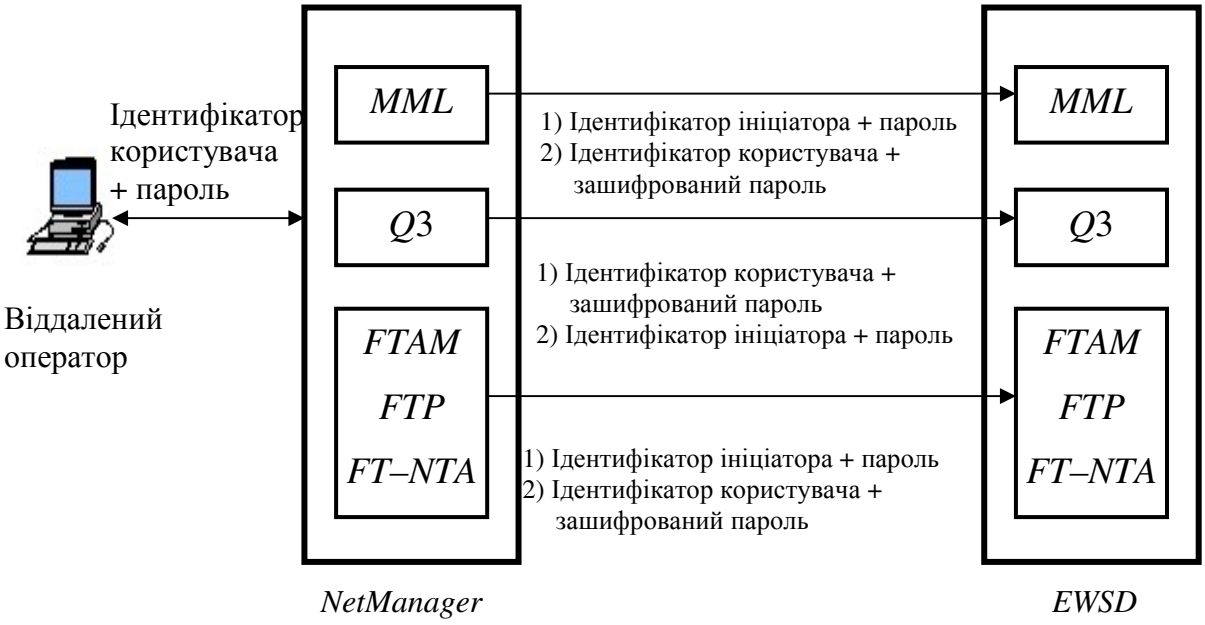

Рисунок 3.3 – Процедури аутентифікації

Захист доступу до даних. Захист доступу до даних запобігає несанкціонованому виконанню команд і несанкціонованому доступу 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 *Q*3-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.

3.3.2 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 встановленню 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 надається виключно одному користувачеві і відомий тільки йому. Паролі повинні складатися принаймні з чотирьох символів та містити принаймні один цифровий символ, один спеціальний символ і одну лутеру.

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 несанкціонованому виконанню *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-ше повноваження. Для запобігання виведення системи з ладу в результаті уведення 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 (рис. 3.4).

Принципи призначення повноважень:

– адміністрування прав доступу Адміністрування *MML* прав дозволяє призначати повноваження користувача і 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 саме правило відноситься і до тих команд, які виконуються за допомогою процесора командних файлів (*COFIP*).

Структура повноважень сеансу показана на рис. 3.5.

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

файла від перезапису чи видалення під час створення запланованого *COFIP*-завдання.

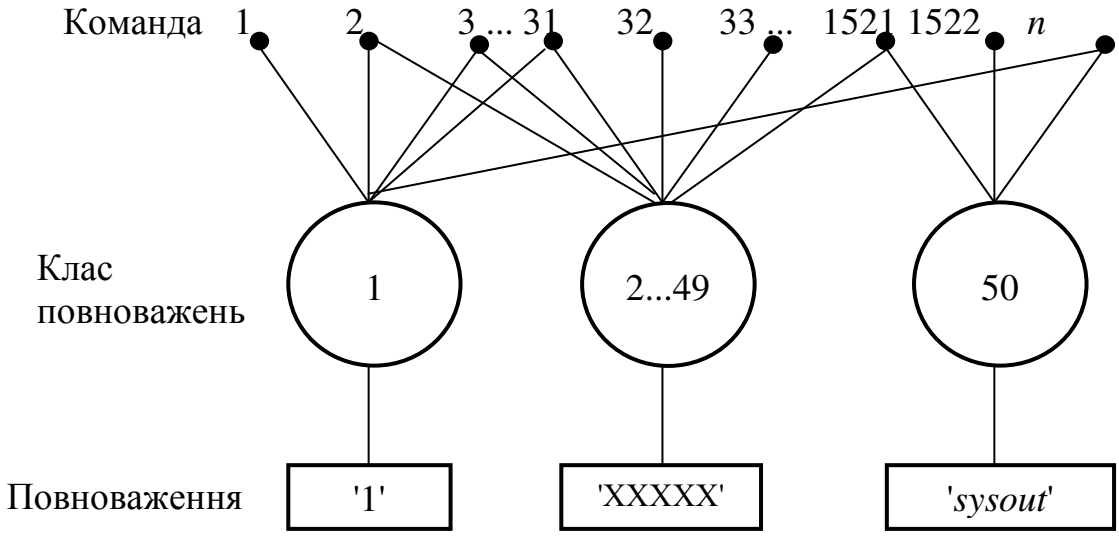

Рисунок 3.4 – Призначення команд повноважень

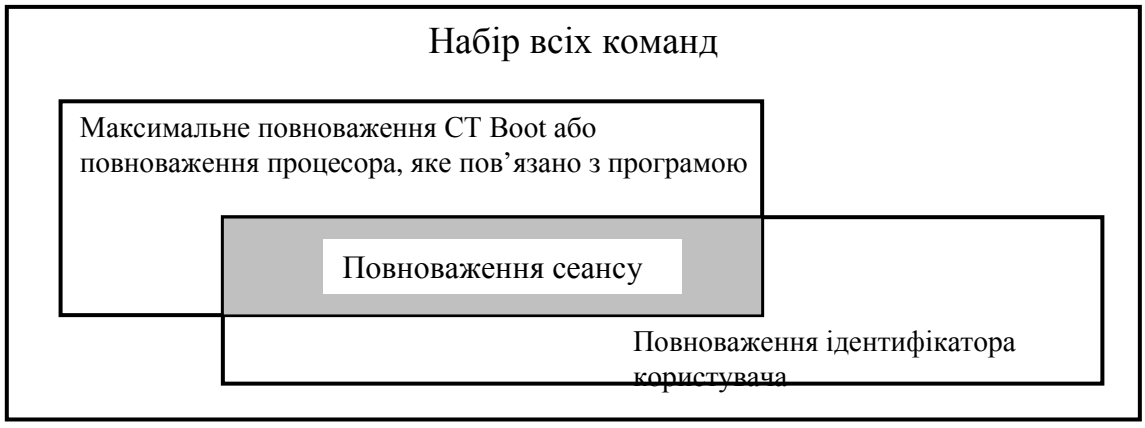

Рисунок 3.5 – Структура повноваження сеансу

Якщо користувач був блокований в період часу між створенням COFIP-завдання і моментом його запланованого виконання, то встановлюється відмінність між ідентифікаторами користувачів, блокованими за командою, введеною оператором, і ідентифікаторами 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 оброблення 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 файли. 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 п’ятий 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 двома 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.

3.3.3 Захист функціонування з використанням Q3

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. 3.6.

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 трасувальник системи захисту);

– виведення аварійних звітів – це функція захисту виведення аварійних звітів (звіт про порушення прав доступу).

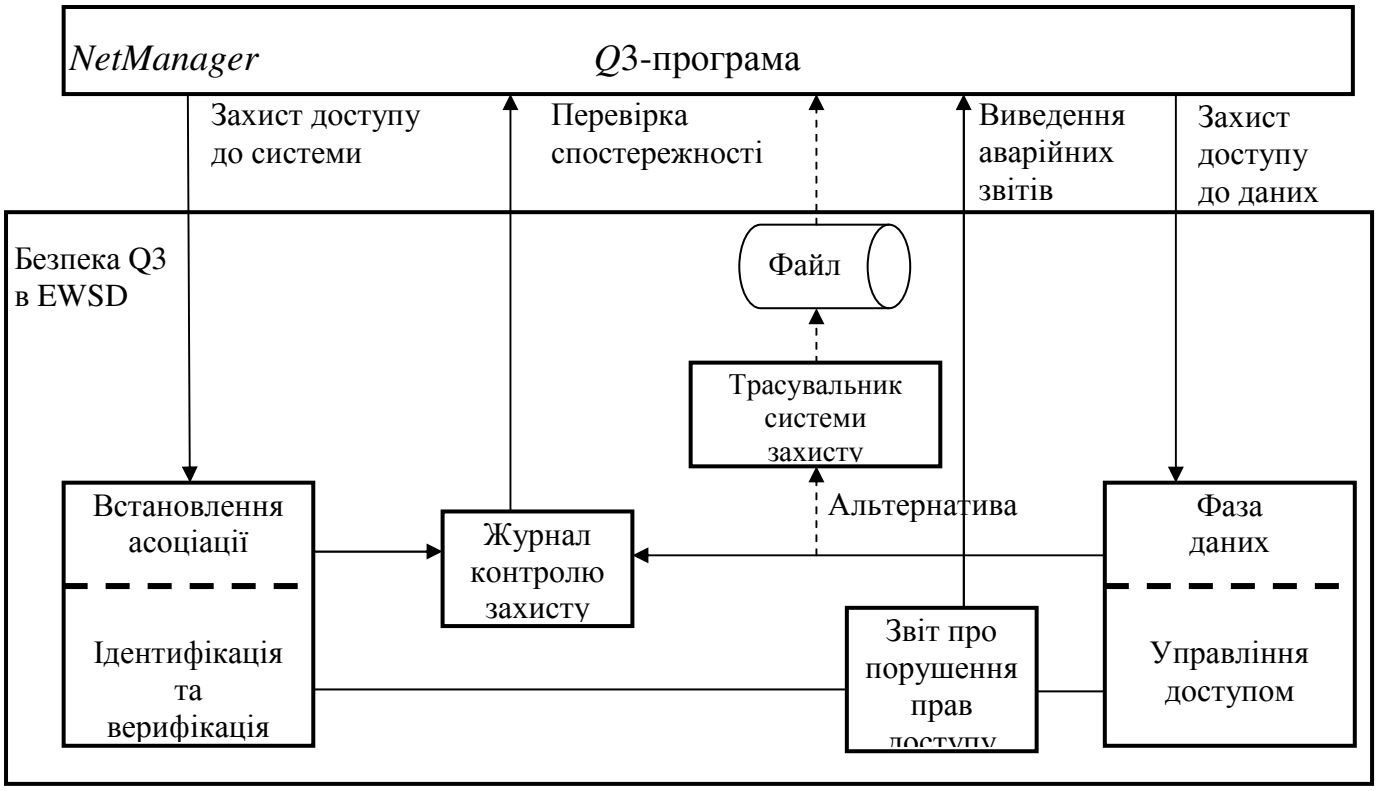

Рисунок 3.6 – Функції *Q*3- захисту

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 відносяться 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 *ОА & М*:

1. 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 позначка і деяке випадкове число, після чого знову використовується функція одностороннього шифрування. Включення тимчасової позначки і випадкового числа забезпечує користувачеві неоднакові результати верифікації пароля для кожного сеансу передавання (захист від спроб використання пароля після завершення з'єднання). Тимчасова позначка і випадкове число також повинні передаватися без шифрування для того, щоб на стороні отримувача також можна було вирахувати результуючу комбінацію.

2. 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 у 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 файла, генеруються відповідні аварійні сигнали. Для аналізу файла з результатами трасування системи захисту потрібна програма пост-оброблення, яка виконується на зовнішньому комп'ютері. Можливе транспортування цього файла 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.

3.3.4 Адміністративна програма для MML-команд

Оброблення 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, описаних в розд. 3 "Захист функціонування з використанням *MML*".

3.3.5 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 розд. 3.3.2.

– виведення аварійних звітів. Контролюються наступні порушення правил доступу: введення невідомих ідентифікаторів користувачів згідно з описом у розд. 3.3.2; введення невірних паролів користувача у відповідності з описом в розд. 3.3.2; несанкціоновані виклики спеціальної програми. Повторні несанкціоновані спроби виконання програми призводять до блокування ідентифікатора у разі досягнення граничного значення.

3.3.6 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 файла, то можливість отримання доступу до нього визначається спільно всіма елементами інформації про захист.

1) *Захист сегментів імен файлів*. Захисту 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 файла, 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 файла; 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 передач вказує, чи був файл успішно скопійований принаймні один раз.

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

– можуть бути в будь-який час змінені;

– ці імена призначаються відповідно до правил, прийнятих в компанії-оператора, а не встановленими у 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 файла.

Захист файлів, пов'язаних з ініціаторами. Повноваження на доступ до файла 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'язаних 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. Звітами про порушення прав доступу є повідомлення, які можуть бути передані і збережені в пам'яті системи.

3.3.7 Захист під час передавання файлів

Засоби захисту під час передавання 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 у віддаленому процесорі-партнері.

Локально ініційований сеанс передачі даних можна запустити тільки в рамках діалогового сеансу *MML*, керування яким виконується механізмами забезпечення захисту *MML* (див. розд. 3.3.2).

У разі дистанційного ініціювання передачі даних спочатку виконується ідентифікація процесора-партнера на основі його мережного адресу. Потім виконується ідентифікація й 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 й аутентифікують їх з використанням простого пароля;

– механізм захисту за допомогою зашифрованих паролів користувача;

– механізм захисту за допомогою зашифрованих паролів ідентифікують за ідентифікатором ініціатора й аутентифікують їх з використанням зашифрованого пароля.

Захист доступу до даних. Для сеансів передачі файлів застосовуються всі механізми захисту файлів, описані у розд. 3.3.6.

Передача файлів можлива тільки в тому випадку, якщо ініціатор має ідентифікатор з повноваженнями на виконання команд передачі даних для локально ініційованих сеансів передачі (див. розд. 3.3.1).

Перевірка спостережності (тільки для FTAM). Вихідні повідомлення, автоматично видаються застосуванням передачі даних *FTAM* для всіх успішно реалізованих сеансів передачі (початок і закінчення), записуються у 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 у розд. 3.3.3;

– введення невірних паролів користувача у відповідності з описом у розд. 3.3.3;

– 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.

3.3.8 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 несуперечливість. Крім того, за допомогою цього застосування виконується розподіл параметрів у мережі передачі даних та їх активізація.

Питання 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 мережному 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 *Q*3?

8. Що таке журнал контролю захисту? Для чого він портрібний?

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

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 оброблення 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 до матеріальних втрат власника або користувача інформації.

Цифрова АТС класифікується згідно з 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, збірання, зберігання, оброблення даних про всі події у 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 факторами, 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 інших 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 оброблення. 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 п. 2.1.3 та 2.2.

4.1.6 Політика безпеки інформації на ЦАТС

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

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

2. 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 оброблення 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 охвату нормативними документами (НД) елементів середовища; повного охвату НД елементів технологій роботи у середовищі та рівня відповідності НД.

Забезпечення спостережності та керованості технологічного середовища залежить від виконання вимог до: ефективності аудиту технологічного середовища; аутентифікації суб'єктів та ідентифікації об'єктів (процесів, ресурсів); 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); реалізації послуг повторного використання об'єктів; захищеності від таємних каналів витоку та каналів спеціального впливу на елементи АТС; фізичної цілісності, розмежування обов'язків та самотестуванню об'єктів.

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

Політика безпеки має бути завершена планом захисту інформації, в 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 підбирання та навчання персоналу і користувачів установленим правилам безпеки інформації, новим методам захисту, підвищення їхньої кваліфікації.

До інженерно-технічних слід відносити заходи, спрямовані на налагодження, випробовування й 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 оброблення 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 розв'язання цієї задачі розробляється система безпеки, основними функціями якої є захист інформації при її обробленні та передаванні 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 частки 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 усередині 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, тому що пов'язана з використанням спеціальних комплексів перехвату. Крім того, проведення таких атак можливе лише за умови розташування апаратури перехоплення в безпосередній близькості від об'єкта, по відношенню до якого проводиться атака.

Але недооцінка загроз витоку інформації каналами ПЕМВН призводить до того, що вони можуть стати самим вразливим місцем у 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 в усій 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 йдуть від моніторів ПЕОМ, а також фізичними лініями. Інші технічні засоби ЦАТС утворюють більш низькі рівні випромінювання. Крім 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, тому що залишаються випромінювання моніторів та фізичних ліній (на неохоплених захистом ділянках), і необхідно використовувати додаткові заходи захисту.

У загальному випадку потрібно вибрати комплекс технічних засобів захисту. При цьому необхідно враховувати низку 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 заходи 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 здібільшого, 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 межі 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 оброблення інформації необхідно виміряти рівень побічних електромагнітних випромінювань та розрахувати радіус зони-2, на межі та за межами якої

відношення сигнал/шум не перевищить нормованого значення. У загальному випадку ця відстань може знаходитись в ближній, перехідній чи дальній зонах. У межах кожної із зон згасання електромагнітної хвилі описується різними аналітичними залежностями. Уміння вірно визначити межі зон необхідне для отримання об'єктивної оцінки величини зони-2.

У даний час межі зон визначаються умовно без достатнього математичного або електродинамічного обґрунтування. Таким чином, при розрахунку радіуса зони-2 допускаються методичні похибки, що неприпустимо при організації захисту інформації обмеженого поширення від витоку за рахунок ПЕМВ. Для багатьох технічних засобів оброблення інформації, наприклад персональних ЕОМ, характерна значна 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 суттєво 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 отримати 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:

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

де ε_a – абсолютна комплексна діелектрична проникність; $A_a = \mu_a I l e^{-ikr}/(4\pi r)$; 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:

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

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

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

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

$$E_\varphi = 0.$$

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 дорівнює 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 дорівнює 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:

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

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

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

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 три 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) набувають виду:

$$E_r = -i\frac{Il}{2\pi\varpi\varepsilon_a}\frac{1}{r^3}\cos\theta;\ \ E_\theta = -i\frac{Il}{4\pi\varpi\varepsilon_a}\frac{1}{r^2}\sin\theta. \qquad (4.5)$$

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:

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

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

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

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

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

Відстанню до межі ближньої зони $r_{бл}$ назвемо відстань від джерела ПЕМВ, на якій максимальна складова E_{m1} у ξ разів перевищує внесок складової E_{m2}. У межах даної відстані можна знехтувати 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 отримати шуканий вираз до межі ближньої зони $r_{бл}=\lambda/(2\pi\xi)$. Аналогічно, для межі дальньої зони отримуємо $r_д=\xi\lambda/(2\pi)$.

Величина прийнятого межевого внеску складових поля ξ залежить від необхідної точності і для практичних розрахунків може складати величину від 3 до 10. На межі ближньої (дальньої) зони можна обмежитися значенням ξ = 3, за якого у виразі (4.4), з урахуванням зведення членів у квадрат, величинами E_{m2} і E_{m3} (E_{m1} і E_{m2}) можна знехтути в порівнянно з E_{m1} (E_{m3}). Так, для ξ = 3 межа ближньої зони складає $r_{бл}=\lambda/(6\pi)$, а межа дальньої зони – $r_д=3\lambda/(2\pi)$.

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 за великих значень 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 межа ближньої зони становить:

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

Межа дальньої зони

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

Ширина перехідної зони

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

Як видно з розрахунків, межа дальньої зони при частоті монітора 110 МГц становить 1,30м. Віддалення границь від джерела ПЕМВ визначається довжиною хвилі та зі збільшенням частоти переміщується в бік джерела. Тому при виборі ПЕОМ для робочого місця оператора з точки зору системи технічного захисту потрібно вибирати монітори з якнайменшою робочою частотою, щоб радіус зони на межі та за межами якої відношення сигнал/шум не перевищив нормованого значення, також 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 установлення з'єднання, управління процесами установлення з'єднання, маршрутизацією та трафіком, в 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-й 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. Позначка, яка присутня в кожному сигнальному повідомленні, використовується для однозначного визначення розмовного каналу, до якого відноситься дане повідомлення.

Система *SS*7 забезпечує надійнє та достовірне передавання 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 ділянок. За спільного режиму роботи для кожного маршруту робочих каналів відводяться сигнальні канали *SS*7 у тому самому маршруті.

За квазіспільного режиму роботи маршрут проходження інформації сигналізації на комутаційній ділянці може не збігатися 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 передаванні інформації *SS*7 обхідними маршрутами можуть використовуватись спільний або квазіспільний режими 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 оброблення у пунктах сигналізації (ПнС) або ТПнС.

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

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

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

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

– обробленням повідомлень сигналізації;

– управлінням мережею сигналізації.

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

Одним із 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 позначкою 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).

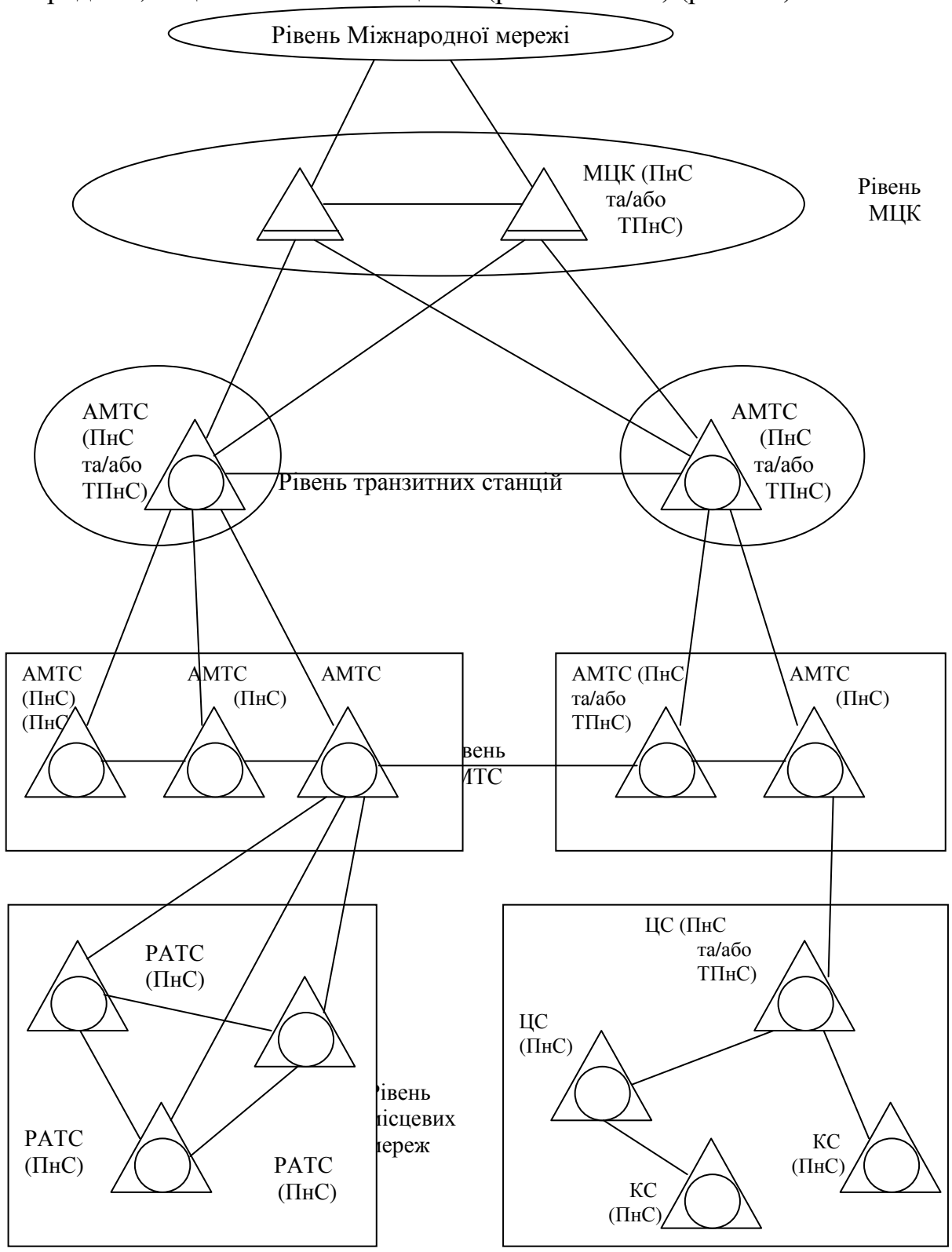

Рисунок 4.1 – Схема багаторівневої мережі *SS*7

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 шлейфовна перевірка розмовних каналів. Шлейфовна перевірка полягає у підключенні до тракту приймально-передавального пристрою на вихідній станції та організації шлейфу 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 с.;

– один канал сигналізації здатний одночасно керувати 2...4 тисячами розмовних каналів;

– економність – порівняно 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 передаванні даних мережею (цілісності даних та цілісності мережі). Захищеність даних від несанкціонованого втручання виявилась порівняно низькою.

4.3.2 Система захисту у мережі SS7

Спочатку мережа *SS*7 створювалася в припущенні, що незначна 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 значна кількість користувачів інших

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

Як уже зазначалося 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, й 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 із 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 централізоване оброблення й 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 незадокументовані 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 отримання 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 у 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 установлених 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 установленого проміжку часу. Така модель справедлива за умов:

– 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 набувати значення у інтервалі від 0 до 1. Якщо функції системи і критерії відмовлення точно задані, то надійність може бути точно виражена кількісно через імовірності.

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

Безвідмовність – це властивість пристрою безперервно зберігати працездатність.

Довговічність – це властивість на заданий термін 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 відмова 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 за одиницю часу після даного моменту часу t за умови, що до цього моменту відмовлення не виникло. Кількісно

інтенсивність відмовлень виражається в числі відмовлень, що припадає на одну годину роботи.

Наробком 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:

$$\lambda = \sum_{i=1}^{n} \lambda_i , \tag{4.13}$$

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 наведемо дані про елементи, що складають ПЕОМ – їх кількість та інтенсивність відмовлень.

Таблиця 4.1 – Інтенсивність відмовлень елементів персональної ЕОМ

Найменування елемента	Кількість елементів одного виду в ПЕОМ, n	Інтенсивність відмовлень одного елемента, λ_e*10^{-6}, 1/год	Сумарна інтенсивність відмовлень елементів одного виду, $n*\lambda_e*10^{-6}$, 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

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 наробка на відмовлення:

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

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

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 наробка на відмовлення T_i.

Якщо знайти середнє значення часу наробка на відмовлення ПЕОМ даної партії, тобто знайти суму наробків на відмову кожної з ПЕОМ і поділити цю суму на кількість ПЕОМ у партії, то отримаємо 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.

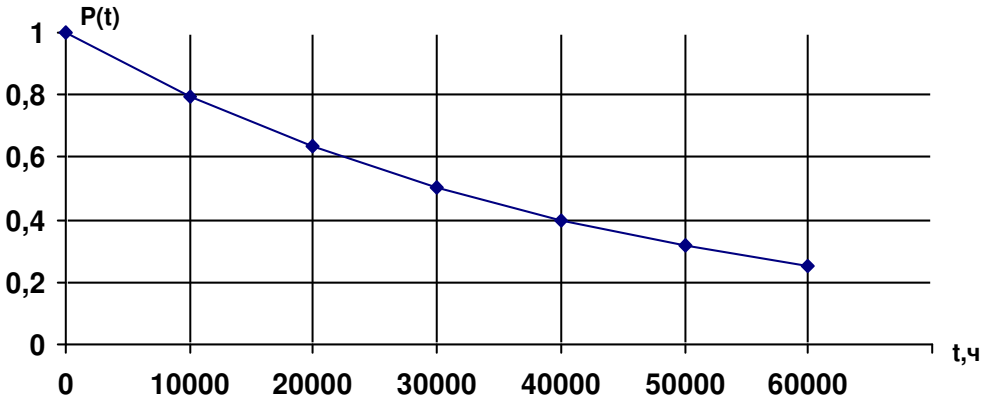

Рисунок 4.2 – Графік залежності ймовірності безвідмовної роботи ПЕОМ у залежності від часу роботи

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.

Наведену методику розрахунку надійності можна застосовувати для широкого кола технічних пристроїв.

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

Метод обмеження фізичного доступу до устаткування зв'язку спрямований 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 запровадженого «закладення», 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 закладення. Такі елементи слід додатково закріплювати й маркувати. Додаткове кріплення й маркування повинні бути непомітні для стороннього спостерігача, але легко перевірятися власником термінала або допущеним обслуговуючим персоналом.

Прокладання проводів, які несуть сигнали незахищеної інформації, повинне виконуватися приховано, за можливості безрознімних з'єднань.

Функційно необхідні розніми 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 нездійсненними, корисним може бути розташування у складі абонентського термінала генераторів електромагнітного шуму. При цьому випромінювальні системи (антени) генераторів повинні бути максимально поєднань 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 обладнання;

– встановлення всього обладнання та елементів інтер'єра має ускладнювати 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 ускладнене 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 суттєво змінюються від примірника до примірника апаратури зв'язку і сполучених з нею виробів, суттєво залежать від впливів, які 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.

Питання 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 інформаційних ресурсів 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 «зломом 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 наробка
на відмовлення та як він обчислюється?

5 ПРОЕКТУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СТАНЦІЇ 5ESS

5.1 Цілі, задачі та принципи інформаційної безпеки

Безпека – це стан захищеності життєво-важливих інтересів підприємства (організації) від потенційно та реально існуючих загроз, або усунення таких загроз, коли дія зовнішніх і внутрішніх факторів не приводить до погіршення або неможливості її функціонування і розвитку.

Інформаційна безпека (ІБ) – це стан захищеності інформації (даних) при всіх її процесах: введення, зберігання, передаванні, перетворення, виведення.

Модель інформаційної безпеки заснована на властивостях інформації:

– конфіденційність інформації (її доступність лише певному колу осіб);

– цілісність інформації (гарантія її існування в початковому вигляді);

– доступність інформації (можливість отримання інформації авторизованим користувачем у потрібний для нього час);

– автентичність інформації (можливість установлення її автора);

– невідмовність (апелятивність) інформації (можливість довести, що автором є саме заявлена людина, і ніхто інший).

Інформаційна безпека досягається активною протидією загрозам.

Тоді як «інформаційна безпека» – це стан захищеності інформації, то «захист інформації» – це діяльність з запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних дій на інформацію, що захищається, тобто процес, спрямовано на досягнення стану захищеності.

Кінцева мета створення режиму інформаційної безпеки – це забезпечення захисту всіх категорій суб’єктів, що прямо або побічно беруть участь у процесах інформаційної взаємодії, від нанесення матеріального, морального або іншого збитку в результаті випадкових або навмисних дій на інформацію і системи її оброблення та передачі. При цьому передбачається створення перешкод для будь-якого несанкціонованого втручання в процес функціонування інформаційної системи.

Несанкціоновані дії – це дії суб’єктів, що порушують установлені в інформаційній системі правил оброблення інформації.

5.1.1 Комплексні системи захисту інформації

Захист сучасних інформаційних систем буде успішним лише при комплексному підході до побудови системи забезпечення ІБ шляхом створення і підтримки комплексної системи захисту інформації.

Комплексна система захисту інформації (КСЗІ) – це сукупність організаційних та інженерно-технічних заходів, які спрямовані на

забезпечення захисту інформації від розголошування, витоку і несанкціонованого доступу.

1) Організаційні заходи включають:

– створення концепції інформаційної безпеки;

– складання посадових інструкцій для співробітників;

– створення правил адміністрування інформаційної системи, обліку, зберігання, розмноження, знищення інформації та її носіїв, ідентифікації користувачів;

– розробка планів дій у разі виявлення атак або спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

– навчання правилам інформаційної безпеки користувачів.

2) Інженерно-технічні заходи – це сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити. Інженерно-технічні заходи включають:

– використання захищених підключень та міжмережних екранів;

– розмежування потоків інформації між сегментами мережі;

– використання засобів шифрування та захисту від несанкціонованого доступу.

У рамках проведення інженерно-технічних заходів, здійснюється установка систем охоронно-пожежної сигналізації, систем контролю й управління доступом. Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

3) Об’єкти захисту КСЗІ – це фактично цінна для підприємства інформація. Залежно від природи, інформаційні сигнали розповсюджуються в певних фізичних середовищах. Залежно від вигляду і форми представлення інформаційних сигналів, які циркулюють у системі, при побудові КСЗІ можуть використовуватися різні засоби захисту.

Цілісний і комплексний підхід до ІБ має на увазі сукупність організаційних і технічних заходів, спрямованих на створення ефективної і сучасної системи ІБ, що забезпечує всебічний захист:

1. Організаційні заходи є етапом розробки структури інформаційної безпеки, підготовкою нормативної бази та регламентуючих документів. Для підвищення ефективності планових заходів на попередньому етапі доцільне проведення аудиту системи інформаційної безпеки.

2. Реалізація технічної політики з забезпечення ІБ повинна виходити з комплексного підходу з системним узгодженням різних елементів, а кожний розроблений елемент розглядатися як частина єдиної системи при оптимальному співвідношенні як технічних, так і організаційних заходів.

3. Організаційно-правовий режим передбачає створення та підтримку правової бази безпеки інформації і розробку (введення в дію) необхідних організаційно-розпорядних документів (положення про зберігання інформації, перелік відомостей складових – службову і комерційну таємницю, накази і розпорядження щодо встановлення режиму

безпеки інформації, інструкції і функціональні обов'язки співробітників та інші нормативні документи).

Інтегрована система ТЗІ – це сукупність організаційно-правових і інженерних заходів, а також програмно-апаратних засобів, які забезпечують ТЗІ у системі. Ця задача розв'язується технічними та програмними засобами базового і прикладного програмного забезпечення, а також з використанням програмних і апаратних засобів ТЗІ, що спеціально розробляються.

Програмні засоби ТЗІ захисту дозволяють створювати захищені системи з побудовою правил розмежування доступу, централізовано управляти процесами захисту, інтегрувати різні механізми та засоби захисту в єдину систему, створювати достатньо зручний інтерфейс адміністратора безпеки.

Процедурний рівень КСЗІ включає заходи щодо забезпечення безпеки, що виконуються службою безпеки та користувачами:

1) управління персоналом;

2) фізичний захист;

3) реагування на порушення режиму безпеки;

4) планування відновних робіт.

Заходи щодо підтримки інформаційних систем:

– підтримка користувачів – питання інформаційної безпеки, виявлення їх типових помилок і забезпечення рекомендаціями;

– підтримка програмного забезпечення, контроль відповідності і сертифікатів;

– конфігураційне управління – контроль змін, що вносяться в програмну і технічну конфігурацію;

– резервне копіювання для відновлення інформаційної системи і даних у випадку аварії та інших обставин непереборної сили;

– управління носіями даних – порядок обліку, обігу та зберігання;

– документування – звіти про поточний стан справ.

Комплексний підхід до створення системи ІБ включає аналіз і оцінку ризиків, зокрема по технічних каналах витоку інформації, облік характеру та важливості інформації, що захищається, контроль над забезпеченням безпеки технології оброблення електронних документів, управління безпекою (постійний контроль за виконанням вимог політики інформаційної безпеки, оперативним внесенням в неї коректувань і підвищення її рівня).

Комплексний критерій оцінки ефективності системи безпеки – це кількісний показник числа та серйозності загроз, захист від яких вона забезпечує. Початкові дані для проектування – це список можливих типів загроз і умови протистояння ним. Знаючи модель несанкціонованого доступу порушника та основні характеристики захищеності, потрібно обрати оптимальний склад КСЗІ. При проектуванні комплексу важливо передбачити можливість удосконалення його у разі потреби внесення змін та уточнень, пов'язаних із загрозами і моделями порушників;

конфігурацією об’єкта і меж, що охороняються; способами захисту; умовами розміщення об’єктів фізичного захисту.

5.1.2 Фізичний захист

Фізичний захист об’єкта виконує охорона та різні види сигналізації, призначені для захисту кожного важливого або цінного об’єкта від вторгнення або несанкціонованого доступу (НСД).

Захист приміщень – це попереджувальний захід від НСД у приміщення. Активним є захист приміщень, що дозволяє попередити або налякати злодіїв: охоронна сигналізація, охоронець і тому подібне. Пасивним захистом є пристосування, що перешкоджають проникненню злодіїв у приміщення: забори, двері із замками, грати на вікнах тощо.

Фізична охорона об’єктів і приміщень – це складова КСЗІ, що безпосередньо виконує дії з виявлення, запобігання та припинення:

– несанкціонованих проникнень на об’єкт охорони;

– перебування осіб без відповідних повноважень на об’єкті охорони;

– протиправного заволодіння майном на об’єкті охорони;

– протиправного використання майна на об’єкті охорони без відповідних повноважень;

– спричинення збитків шляхом навмисного пошкодження або знищення майна, протиправних посягань на персональну безпеку осіб, їх недоторканність.

Фізичний захист повинен здійснюватися за принципами: законність; захист; активність; економічна доцільність; безперервність; конкретність; професіоналізм. Головні завдання фізичного захисту об’єктів і приміщень:

– охорона матеріальних цінностей, здійснення контрольно-пропускного режиму, забезпечення регламенту діяльності, протипожежний контроль;

– контроль співробітників і відвідувачів, нагляд за приміщеннями та територією, підтримка порядку; припинення спроб розкрадання матеріальних цінностей та несанкціонованого винесення документів і майна з території об’єкта;

– забезпечення громадського порядку на території, що охороняється, та прилеглій території, нагляд за приміщеннями шляхом патрулювання території з періодичним оглядом важкодоступних ділянок (підвальних і горищних приміщень) або за допомогою технічних засобів (систем відео-нагляду, сигналізації тощо);

– охорона приватної власності, нагляд за рухом автотранспорту.

Фізична охорона об’єктів і приміщень включає:

1. Охорону периметра, стаціонарні пости охорони.

2. Охоронну сигналізацію комплексної системи безпеки, до складу якої входить: обладнання управління охоронною сигналізацією; приймально-контрольні прилади для збирання й оброблення інформації з датчиків; датчики.

Охоронна сигналізація інтегрується в КСЗІ, забезпечуючи достовірною інформацією системи сповіщення, відео нагляду та контролю доступу.

Рівень захищеності не однаковий для різних за призначенням об'єктів, унаслідок чого потрібна їх класифікація за групами. Як основний критерій у визначенні категорії об'єкта виступає тип і цілі захисту. Для кожної групи об'єктів слід визначити основні характеристики, що впливають на показник захищеності об'єкта: кількість каналів і способів проникнення; кількість рубежів захисту й охорони; ймовірність виявлення порушників технічними засобами, встановленими на рубежах охорони, їх надійність.

Захист приміщень і об'єктів крім фізичного захисту є важливим засобом інформаційного захисту, оскільки запобігає НСД в приміщення та на об'єкти зловмисників, які могли б спробувати установити підслуховуючу техніку або інші пристрої для збирання інформації.

Практика показує, що суворе дотримання всього комплексу заходів фізичної безпеки в поєднанні з особистою зацікавленістю співробітників і охорони створить неперебornий бар'єр для зловмисників, для яких небезпека швидкого викриття їх злочинних дій на об'єкті буде сильнішим за бажання отримати будь-кі особисті вигоди.

5.1.3 Робота з кадрами по захисту інформації

Кадрова політика відносно захисту інформації – найважливіша частина КСЗІ. Найнадійніша КСЗІ неефективна при помилці обслуговуючого працівника. *Кадрова безпека* – це процес запобігання негативним діям на безпеку підприємства за рахунок усунення або зниження ризиків і загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими взаємостосунками в цілому.

Слід розрізняти зовнішні і внутрішні кадрові ризики. Зовнішні негативні дії – це дії, явища або процеси, не залежні від волі й свідомості співробітників підприємства та спричиняють нанесення збитку. Внутрішні негативні дії – це дії (умисні або необережні) співробітників підприємства, що також ведуть до нанесення збитку.

Внутрішні кадрові небезпеки такі:

– невідповідність кваліфікації співробітників;
– недостатня кваліфікація співробітників;
– слабка організація системи управління персоналом;
– слабка організація системи навчання;
– неефективна система мотивації;
– помилки в плануванні ресурсів персоналу;
– зниження кількості ініціатив (раціоналізаторських пропозицій);
– витік кваліфікованих співробітників;
– орієнтування на вирішення лише дрібних тактичних задач;
– дотримання лише внутрішніх інтересів підрозділу;
– слабка корпоративна політика;

– неякісні перевірки кандидатів при прийомі на роботу.

До зовнішніх кадрових небезпек відносяться:

– кращі умови мотивації у конкурентів;

– установка конкурентів на переманювання;

– дія на співробітників ззовні;

– зміни в зовнішній економічній ситуації;

– попадання співробітників в різні види залежності;

– інфляційні процеси і глобальні економічні зміни.

Кадрова безпека залежить від трьох головних чинників:

1) Перевірка при прийомі на роботу (тестування, прогнозування благонадійності і відбір) – це розгляд питань безпеки підприємства при пошуку кандидатів, відборі, документальному і юридичному забезпеченні прийому співробітника на роботу, випробувальний термін, навчання і адаптація, а також навчання на основі атестацій.

2) Лояльність – це заходи щодо встановлення позитивних відносин кожного співробітника до працедавця, він повинен відчувати себе потрібним членом команди.

3) Контроль – це заходи щодо регламентації, встановлення правил, обмежень і режимів технологічних процесів, а також процедур безпеки. Цей комплекс заходів спрямовано на ліквідацію можливостей спричинення збитку і відпрацьовується службою безпеки спільно з відділом кадрів.

Головними групами критеріїв кадрової безпеки можна назвати:

– показники чисельного складу штату, його динаміки і плинність;

– показники кваліфікації й інтелектуального потенціалу;

– показники ефективності використання персоналу;

– показники якості мотиваційної системи.

Ще один аспект кадрової політики безпеки – це «групи ризику». Вкрай небажана присутність в колективі працівників, які входять або можуть увійти до групи ризику. Актуальні такі залежності, як наркотична, алкогольна, комп’ютерна та сексуальна.

Загальні заходи запобігання негативним впливам груп ризику для безпеки підприємства полягають у: надійному вхідному контролі пристрастей та залежностей (анкетування, перевірка відомостей, співбесіда з метою виявлення ознак поведінки); контролі під час терміну випробування працівника. Крім того, в кадровій безпеці актуальні також питання дотримання трудової дисципліни і законності, підвищення культури співробітників підприємства.

Для забезпечення кадрової безпеки потрібно уникати помилок: байдужості до долі співробітників; небажання керівництва та служби безпеки займатися роботою з підлеглими; відсутність у керівників навиків роботи з кадрами. Усунення цих причин можливе підвищенням компетентності керівництва і внесення в посадові інструкції керівників конкретних обов’язків по роботі з кадрами і контролю їх дотримання.

5.2 Загальна архітектура й основні технічні параметри системи комутації 5ESS

Електронна цифрова система комутації 5ESS розроблена фірмою AT&T, має гнучку розподілену структуру обладнання та програмного забезпечення (ПЗ) і є універсальною за можливостями використання на існуючих і перспективних телекомунікаційних мережах. Архітектура 5ESS (рис. 5.1) в опорному обладнанні складається з: комутаційних модулів SM (Switching Modules), модуля комунікацій CM (Communication Module) та модуля управління й експлуатації AM (Administrative Module).

Комутаційний модуль SM – основна одиниця нарощення ємності системи. До SM приєднують абонентські (ААЛ) та зовнішні SS з'єднувальні лінії (ЗЛ). SM виконує функції з обслуговування викликів, забезпечуючи комутацію каналів і комутацію пакетів. Внутрішнє навантаження замикається в SM, а з'єднання між ААЛ і ЗЛ, ввімкненими в різні SM, встановлюються через модуль комутації CM по внутрішньо системних волоконно-оптичних лініях зв'язку, керування та синхронізації, так званих лініях NCT (Network, Control and Timing links). Між CM і кожним SM чотири двоволоконні лінії NCT (дві резервні) зі швидкістю передавання інформації в кожній 32,768 Мбіт/с. Модуль SM комутує максимум 512 × 512 часових каналів, а між SM і CM – 512 основних і 512 резервних каналів. Нова модифікація модуля (SM-2000) має просторово-часовий комутатор на 12288 × 12288 точок комутації.

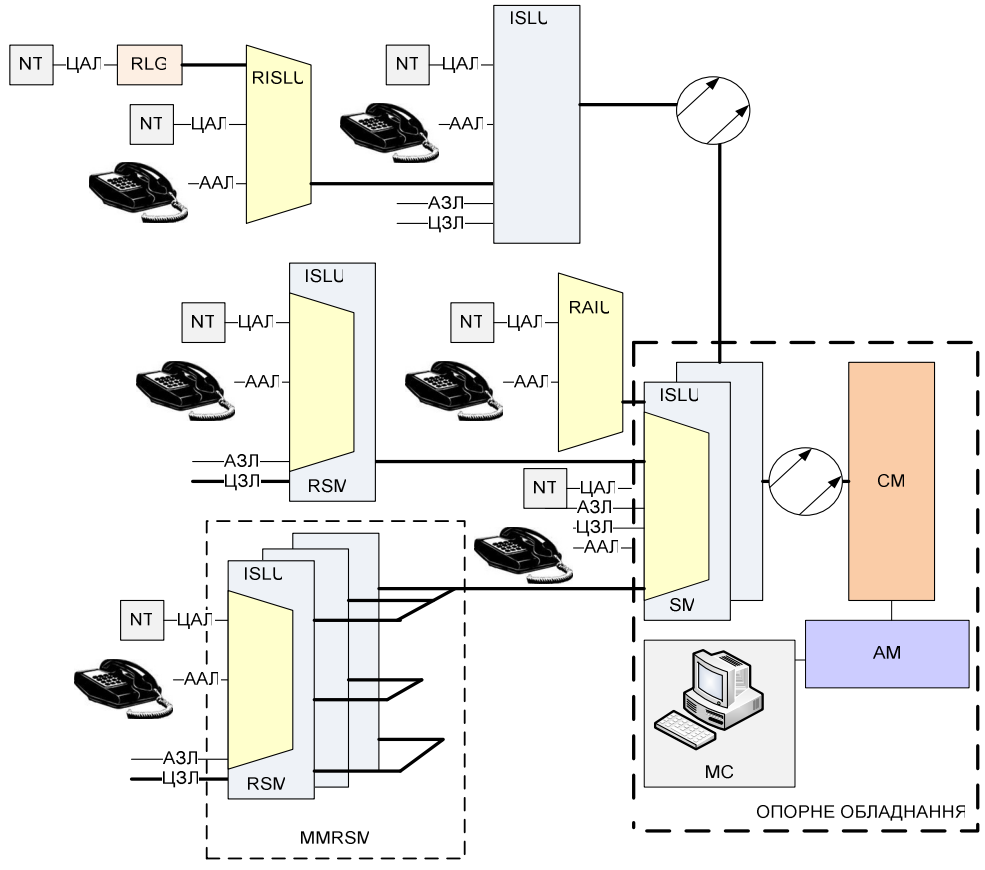

Рисунок 5.1 – Загальна архітектура ЦСК 5ESS

Модуль SM (але не SM-2000) може знаходитись зовні приміщення опорного обладнання (ОпО) системи. Такий виносний комутаційний модуль (RSM – Remote SM) може мати прямі зв'язки з іншими RSM і в телекомунікаційній мережі фактично виконує всі функції самостійної АТС. В бік опорного обладнання (Host) RSM він має до 16 стандартних 32-канальних лінійних трактів ІКМ зі швидкістю передавання 2048 кбіт/с (ЛТ 2048), організованих у будь-якому середовищі розповсюдження (мідні, коаксіальні або волоконно-оптичні кабелі, радіо-релейні чи супутникові лінії зв'язку). Ці тракти приєднуються до локального SM (або SM-2000) опорного обладнання. При оптичних лініях довжиною до 300 м RSM безпосередньо з'єднується з модулем комутації СМ. До чотирьох RSM можуть об'єднуватись у багатомодульний виносний комутаційний модуль MMRSM (MultiModule RSM).

Абонентські лінії двопроводові, з припустимим опором шлейфу (з урахуванням ТА) до 2 кОм. Вони безпосередньо вмикаються в інтегральні блоки абонентських ліній ISLU (Integrated Services Line Unit) або в інтерфейсні блоки доступу AIU (Access Interface Unit), що входять до складу SM. Ці блоки можуть бути і виносними (RISLU – Remote ISLU, RAIU – Remote AIU), розміщуваними в місцях концентрації абонентів. Замикання внутрішнього навантаження в них не передбачено. Між RISLU та SM (RSM) утворюється від 4 до 24 лінійних трактів 2048 кбіт/с в будь-якому середовищі розповсюдження. Від ISLU (RISLU) за допомогою трактів 2048 кбіт/с можливе додаткове винесення групового обладнання 32 чи 64 аналогових або цифрових АЛ, так званої виносної абонентської групи RLG (Remote Line Group). Припустимі відстані між RISLU і SM (RSM) та між RSM і опорною станцією – до 160 км.

До кожного ISLU2 приєднується до 2048 індивідуальних аналогових (ААЛ) чи до 1024 цифрових АЛ (ЦАЛ). Для аналогових АЛ виконуються функції BORSCHT, для цифрових надається основний доступ (BRA – Basic Rate Access) до цифрової мережі з інтеграцією служб (ЦМІС), тобто канали 2B + D16 ($2 \times 64 + 16 = 144$ кбіт/с). Функції блоків AIU такі ж, як ISLU, але завдяки новій технології ємність абонентських плат збільшена до 32 ААЛ чи 12 ЦАЛ і тому загальна ємність блоку досягає 3584 ААЛ чи 1440 ЦАЛ.

В SM може бути до 8 ISLU (AIU) чи RISLU (RAIU), але при цьому загальна кількість АЛ для SM не повинна перевищувати 5120 аналогових або 2048 цифрових. В цілому SM має шістнадцять 32-канальних групових трактів для з'єднання ISLU (AIU), RISLU (RAIU) та зовнішніх цифрових ЗЛ. Оскільки пропускна здатність модуля обмежена величиною 450 Ерл, то реально припустима кількість АЛ і ЗЛ відчутно менша за граничні значення й визначається при проектуванні в залежності від конкретних умов і прогнозованих інтенсивностей навантажень. Реальна ємність SM (RSM) становить 2000…4000 АЛ, а ємність чотиримодульного MMRSM не перевищує 14000 АЛ. Для SM-2000 припустима ємність зростає більш ніж вдесятеро і становить, залежно від конкретних умов, від п'ятнадцяти до п'ятидесяти тисяч АЛ.

Модуль комутації СМ за допомогою блока просторової комутації TMS та комутатора повідомлень MSGS відповідно забезпечує комутацію каналів між SM і комутацію пакетів для обміну управляючими повідомленнями між процесорами SM або SM і AM. У залежності від кількості установленого обладнання модуля комутації СМ можна мати від 30 до 190 SM або від 32 до 192 комутаційних модулів у комбінації SM і RSM.

Розподілене програмне керування забезпечується потужними 32-розрядними мікропроцесорами. Функції управління виконує модуль управління й експлуатації АМ. У розпорядженні персоналу є різноманітні пристрої введення і зберігання інформації, які приєднуються до модуля АМ: накопичувачі на магнітній стрічці (НМС) та на жорстких магнітних дисках (НМД), принтери і відео-термінали з клавіатурою для введення управляючих директив і даних. На їх основі утворюється головний центр управління системою МСС (Master Control Center), який може знаходитись у приміщенні опорної станції або бути виносним.

У разі потреби ЦСК обладнується багатофункційною системою технічного обслуговування MFOS (MultiFunction Operations System), що являє собою комплекс обладнання (спеціалізовані за функціями комп'ютери та відеотермінали робочих місць персоналу, засоби акустичної та візуальної аварійної сигналізації, принтери, накопичувачі на магнітних дисках і стрічці, модеми для приєднання винесених терміналів), з'єднаного локальною мережею передачі даних. На базі MFOS створюється центр технічної експлуатації ОМС (Operations & Maintenance Center), що виконує функції технічного обслуговування, експлуатації й адміністративного керування (OA&M – Operations, Administration & Maintenance functions) всіма наявними на національній мережі системами 5ESS. Модулі АМ обслуговуваних ЦСК з'єднується з MFOS дискретним каналом зі стиком X.25. Кожна з цих ЦСК може функціонувати без постійної присутності персоналу – тоді у разі потреби (пошкодження тощо) MFOS автоматично викликає персонал у потрібне місце за допомогою засобів електронної пошти та пейджерного зв'язку.

Універсальність 5ESS, з точки зору використання на мережах зв'язку, забезпечується:

– модульною архітектурою обладнання та програмного забезпечення;

– широким діапазоном ємностей – від кількох сотень до 300000 АЛ;

– широкою номенклатурою послуг, що надаються абонентам – як традиційних телефонних, так і послуг ЦМІС;

– можливостями комутації каналів і пакетів та квазіширокосмугової комутації 32-канальних трактів;

– можливістю безпосереднього доступу до транспортної мережі на рівні синхронного транспортного модуля STM1 (Synchronous Transport Module), тобто на швидкості 155 Мбіт/с ;

– здатністю утворювати стільникову мережу рухомого радіотелефонного зв’язку у стандартах GSM-900, DCS-1800, CDMA-IS-95;

– наявністю різноманітних способів міжстанційної взаємодії, зокрема багаточастотного коду “два з шести”, системи сигналізації R2D, декадного коду, спільних каналів сигналізації СКС № 7.

Універсальність 5ESS дозволяє застосовувати її обладнання в якості: опорної (ОПС), транзитної (ТС) або опорно-транзитної (ОПТС) станції міської телефонної мережі (МТМ); міжміської або міжнародної АТС; центру комутації стільникової мережі радіотелефонного зв’язку з рухомими об’єктами; а також “шлюзової” (gateway) станції для взаємодії з різними спеціалізованими мережами – передавання даних з комутацією каналів або пакетів, локальними обчислювальними мережами та іншими.

5.3 Обстеження та аналіз вузла комутації, що захищається

Створення комплексної системи захисту інформації (КСЗІ) складається з декількох етапів, перший з яких – аналіз об’єкта. На основі цього аналізу складається план реалізації КСЗІ для конкретної ситуації, в даному випадку – для вузла комутації мобільного оператора, що використовує як телефонну станцію («комутатор») 5ESS.

Задача: Необхідно захистити інформацію в приміщенні, в телекомунікаційній і корпоративній (комп’ютерній) мережі вузла комутації мобільного оператора, що використовує телефонну станцію 5ESS.

5.3.1 Загальний аналіз вузла комутації

Загальні відомості про вузол комутації:

Форма власності: товариство з обмеженою відповідальністю.

Кількість співробітників: 12.

Вид діяльності: мобільний зв’язок.

Підприємство має прямі контракти з абонентами та іншими телекомунікаційними компаніями.

Приміщення підприємства займають п’ять кімнат на першому поверсі.

Ступінь конфіденційності оброблюваної інформації: суворо конфіденційно. Кожен інженер вузла комутації працює з конфіденційною інформацією. Серед документів, доступ до яких необхідно обмежити, виділяються: технічна інформація про вузол комутації; інформація про абонентів; інформація щодо каналів, трафіка та оточення вузла.

Висота стель: 3,28 м. Стеля – підвісна гіпсокартонна, повітряний зазор: 0,2 м. Перекриття підлоги, стелі: залізобетонні, паркет: ламінат.

Стінні перегородки: цегляні. Цеглина – силікатна. Стіни зовнішні: піноблоки, товщина – 0,7 м.

Вікна: розмір отвору – 2,60 × 1,40 м, кількість отворів – 6. Тип вікна – з подвійним склом, товщина скла 3 мм.

Двері: розмір отвору: 2,20 × 1,40 м, двостулкові без ущільнень; замок захищено від злому.

Опис суміжних приміщень: поверх зверху – приміщення, що орендуються іншими компаніями; знизу – підвал.

Розташування будівлі: північ – торцева сторона будівлі, південь – внутрішній двір, захід – фасад будівлі, схід – тильна сторона будівлі.

Система електроживлення: мережа 380/220 В. Система заземлення: є.

Система вентиляції: кондиціонери. Система опалювання: центральне водяне, 4 стояки, що проходять знизу до верху.

Тип обладнання вузла комутації: АТС типу 5ESS виробництва Alcatel-Lucent (колишня назва – Lucent Technologies), версія ПО – 16.1

Об’єкт розташовано в діловій частині міста, з усіх боків оточено спорудами комерційного призначення. Об’єкт оточено з усіх боків проходами, що дає можливість візуального огляду. З північної сторони на відстані 55 метрів розташована 5-поверхова будівля. Із західної – на відстані 32 метрів від об’єкта проходить автодорога. З південної – на відстані 17 метрів розташована сусідня будівля. З східного боку на відстані 29 метрів від об’єкта проходить автодорога. Всі вікна об’єкту, що захищається, виходять на захід і схід.

Всі описані дані наносять на плани будівлі та поверху.

5.3.2 Виявлення каналів витоку інформації

Найбільшу увагу слід приділити технічним каналам витоку інформації, оскільки їх число значне, і внутрішнім каналам витоку («людському чиннику»), оскільки їх наслідки можуть бути катастрофічними.

Технічний канал витоку інформації – це сукупність об’єкта захисту, технічного засобу розвідки, за допомогою якого здобувається інформація щодо об’єкта, та фізичного середовища, в якому розповсюджується інформаційний сигнал.

Канал витоку інформації показує спосіб отримання захищеної інформації за допомогою технічного засобу. *Сигнали* – це матеріальні носії інформації, і за своєю фізичною природою сигнали можуть бути електричними, електромагнітними, акустичними тощо.

Технічні засоби приймання, оброблення, зберігання та передавання інформації – це технічні засоби, що безпосередньо обробляють конфіденційну інформацію. До таких засобів, що захищаються, відносяться: АТС; комп’ютери; обладнання локальної мережі.

При виявленні технічних каналів витоку інформації на об’єкті (вузлі комутації на базі станції 5ESS) необхідно розглядати об’єкт як систему, що включає основне обладнання, прикінцеві пристрої, з’єднувальні лінії (сукупність зовнішніх кабелів і кабелів, прокладених між елементами системи), розподільне обладнання та крос, системи електроживлення, система заземлення.

Об'єкт захисту – технічні засоби, призначені для оброблення конфіденційної інформації, разом з приміщеннями, в яких вони розміщуються. Разом з технічними засобами роботи з інформацією, в приміщеннях установлюються допоміжними технічні засоби – технічні засоби і системи, що безпосередньо не беруть участь в обробленні конфіденційної інформації, але що використовуються сумісно і що знаходяться в зоні електромагнітного поля. До них відносяться: системи пожежної і охоронної сигналізації, електромережа, електропобутові прилади і подібне.

Як канали витоку найбільш небезпечні допоміжні технічні засоби, що мають вихід за межі контрольованої зони об'єкта, тобто що виходять за зону, в якій виключено появу сторонніх осіб.

Крім з'єднувальних ліній (кабелів) основних і допоміжних технічних засобів за межі контрольованої зони можуть виходити дроти і кабелі, які до них не відносяться, але проходять через приміщення, де установлені технічні засоби, а також металеві труби систем опалювання, водопостачання й інші струмопровідні металоконструкції. Такі дроти, кабелі і струмопровідні елементи називаються *сторонніми провідниками*.

До електромагнітних каналів витоку інформації відносяться канали витоку інформації, що виникають за рахунок різного виду побічних електромагнітних випромінювань і наведень (ПЕМВН):

– випромінювань елементів технічних засобів передачі інформації;

– випромінювань на частотах роботи високочастотних генераторів.

У технічних засобах передачі інформації носієм інформації є електричний струм, сила струму (напруга), частота і фаза якого змінюються за законом інформаційного сигналу. При проходженні електричного струму струмо-ведучими елементами навкруги них у навколишньому просторі виникає електричне і магнітне поля. Через це елементи інформаційної системи стають випромінювачами електромагнітного поля, модульованого з згідно із законом зміни інформаційного сигналу.

Електромагнітні випромінювання на частотах роботи високочастотних генераторів технічних засобів передачі інформації (ТЗПІ) і допоміжних технічних засобів (ДТЗ) викликані тим, щодо складу і перших, і других входять різні високочастотні генератори. В результаті зовнішніх дій інформаційного сигналу (наприклад, електромагнітних коливань) на елементи ВЧ-генераторів наводяться електричні сигнали. Приймачем магнітного поля можуть бути котушки індуктивності коливальних контурів, дроселі в ланцюгах електроживлення і таке інше; приймачем електричного поля можуть дроти високочастотних ланцюгів й інші елементи. Наведені електричні сигнали можуть викликати ненавмисну модуляцію власних ВЧ-коливань генераторів. Ці модульовані ВЧ-коливання випромінюються в навколишній простір.

Перехоплення побічних електромагнітних випромінювань від ТЗПІ здійснюється засобами радіотехнічної розвідки, розміщеними за межами контрольованої зони.

Причинами виникнення електричних каналів витоку інформації є:

– наведення електромагнітних випромінювань ТЗПІ на з'єднувальні лінії ДТЗ і сторонні провідники, що виходять за межі контрольованої зони;

– витік інформаційних сигналів в ланцюзі електроживлення ТЗПІ;

– витік інформаційних сигналів в ланцюзі заземлення ТЗПІ.

Наведення електромагнітних випромінювань ТЗПІ виникають при випромінюванні елементами ТЗПІ (у тому числі і їх з'єднувальними лініями) інформаційних сигналів, а також за наявності гальванічного зв'язку з'єднувальних ліній ТЗПІ і сторонніх провідників або ліній ДТЗ. Рівень сигналів, що наводяться, значною мірою залежить від потужності випромінюваних сигналів, відстані до провідників, а також довжини сумісного пробігу з'єднувальних ліній ТЗПІ і сторонніх провідників.

Випадкова антена – це ланцюг ДТЗ або сторонній провідник, що здатний приймати побічні електромагнітні випромінювання:

– зосереджена випадкова антена є компактним технічним засобом, наприклад телефонний апарат або подібне;

– розподілена випадкова антена, це антена з розподіленими параметрами: кабель, дріт, металева труба та струмо-провідник.

Технічне знімання інформації можливе також з використанням апаратних закладок («*заставних пристроїв*») – електронних пристроїв перехоплення інформації. Вони є міні-передавачами, випромінювання яких модулюється інформаційним сигналом. Перехоплена за допомогою заставних пристроїв інформація або безпосередньо передається радіоканалом, або спочатку записується на спеціальний пристрій, що запам'ятовує, а вже потім за командою передається на об'єкт, що запитав її.

Перехоплення оброблюваної в технічних засобах інформації можливе також шляхом їх «високочастотного опромінювання». При взаємодії опромінюючого електромагнітного поля з елементами ТЗПІ відбувається перевипромінювання електромагнітного поля. У ряді випадків це вторинне випромінювання модулюється інформаційним сигналом. При зніманні інформації для виключення взаємного впливу сигналів, що опромінюють та перевипромінють, може використовуватися їх тимчасова або частотна розв'язка. Для опромінювання ТЗПІ можуть використовувати імпульсні сигнали. При перевипромінюванні параметри сигналів змінюються, тому даний канал витоку інформації називають *параметричним*. Для перехоплення інформації за даним каналом необхідні спеціальні високочастотні генератори з антенами, що мають вузькі діаграми спрямованості і спеціальні радіоприймальні пристрої.

Акустична інформація – це інформація, носієм якої є акустичні сигнали. *Мовна інформація* – це акустична інформація, джерелом якої є людська мова. Акустичний сигнал є коливаннями пружного середовища,

що виявляються у виникненні акустичних хвиль різної форми і тривалості. *Акустичні хвилі* – механічні коливання частинок пружного середовища, що розповсюджуються від джерела коливань в навколишній простір у вигляді хвиль різної довжини. *Мовний сигнал* – це складний акустичний сигнал (що включає цілий спектр гармонік) у діапазоні частот 300...6000 Гц.

Первинними джерелами акустичних коливань є органи мови людини, а вторинними – перетворювачі різного типу, зокрема електроакустичні. Вони є пристроями, призначеними для перетворення акустичних коливань в електричні і навпаки. До них відносяться мікрофони, телефони, гучномовці й інші пристрої.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища розповсюдження акустичних коливань і способів їх перехоплення технічні канали витоку акустичної (мовної) інформації можна поділити на повітряні, вібраційні, електроакустичні, оптико-електронні і параметричні.

У повітряних технічних каналах витоку інформації середовищем розповсюдження акустичних сигналів є повітря, і для їх перехоплення використовуються мініатюрні високочутливі мікрофони та спеціальні направлені мікрофони. Мініатюрні мікрофони з'єднуються з портативними звукозаписними пристроями (диктофонами) або спеціальними мініатюрними передавачами. Автономні пристрої, що конструкційно об'єднують мініатюрні мікрофони і передавачі, називають заставними пристроями перехоплення мовної інформації («*акустичними закладками*»).

Перехоплена заставними пристроями мовна інформація може передаватися по радіоканалу, по мережі змінного струму, з'єднувальним (телекомунікаційним) лініям ВТС, стороннім провідникам (трубам опалювання, водопостачання або каналізації, металоконструкціям і тому подібному). Для передавання інформації по трубах і металоконструкціях можуть використовуватися не лише електромагнітні, але й механічні ультразвукові коливання.

У вібраційних технічних каналах витоку інформації середовищем розповсюдження акустичних сигналів є конструкції будівлі (стіни, стелі, підлоги), труби водопостачання, опалювання або каналізації та інші тверді тіла. Для перехоплення акустичних коливань в цьому випадку використовуються контактні мікрофони («стетоскопи»). По вібраційному каналу також можливе перехоплення інформації з використанням заставних пристроїв.

Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні і включають перехоплення акустичних коливань через ДТЗ, що мають «мікрофонний ефект», та «високочастотним нав'язуванням».

Деякі елементи ДТЗ, зокрема трансформатори, котушки індуктивності, електромагніти дзвінків телефонних апаратів, дроселі ламп денного світла, реле і тому подібне, володіють властивістю змінювати свої параметри (ємність, індуктивність, опір) під дією акустичного поля,

створюваного джерелом акустичних коливань. Зміна параметрів приводить або до появи на даних елементах ЕДС, що змінюється згідно із законом впливаючого інформаційного акустичного поля, або до модуляції струмів, що протікають цими елементами, інформаційним сигналом. Наприклад, акустичне поле, впливаючи на якір електромагніту викликуваного телефонного дзвінка, викликає його коливання, внаслідок чого змінюється магнітний потік осердя електромагніту; зміна цього потоку викликає появу ЕДС самоіндукції в котушці дзвінка, що змінюється за законом зміни акустичного поля.

ДТЗ, крім того, можуть містити безпосередньо електроакустичні перетворювачі; до них відносяться гучномовці. Ефект електроакустичного перетворення акустичних коливань в електричні називають *мікрофонним ефектом*. Перехоплення акустичних коливань у даному каналі витоку інформації здійснюється шляхом безпосереднього підключення до з'єднувальних ліній ДТЗ, що мають мікрофонний ефект, спеціальних високочутливих низькочастотних підсилювачів. Наприклад, підключаючи такі засоби до з'єднувальних ліній телефонних апаратів з електромеханічними дзвінками, можна прослуховувати розмови, що відбуваються в приміщеннях, де встановлені ці апарати. Такий канал витоку інформації використовується для перехоплення розмов, що ведуться в приміщенні, через телефонний апарат, лінія якого виходить за межі контрольованої зони.

Оптикоелектронний («лазерний») канал витоку акустичної інформації утворюється при опромінюванні лазерним променем вібруючих в акустичному полі тонких поверхонь, що відбивають (скло вікон і таке інше). Відбите лазерне випромінювання модулюється за амплітудою та фазою (за законом вібрації поверхні) і приймається приймачем оптичного (лазерного) випромінювання, при демодуляції якого виділяється мовна інформація. Для перехоплення мовної інформації цим каналом використовуються лазерні акустичні локаційні системи, називані *лазерними мікрофонами*. Працюють вони в інфрачервоному діапазоні хвиль.

Інформація може передаватися каналами зв'язку (телефонними каналами, комп'ютерною мережею), де перехоплюється. Сьогодні для передавання інформації використовують в основному кабельні лінії зв'язку:

1. Електромагнітні випромінювання передавачів засобів зв'язку, модульовані інформаційним сигналом, можуть перехоплюватися портативними засобами радіорозвідки і за необхідності передаватися в центр оброблення для їх розкодування. Даний канал перехоплення інформації найбільш ширше використовується для прослуховування телефонних розмов, що відбуваються по радіотелефонах, стільникових телефонах.

2. Електричний канал перехоплення інформації, що передається кабельними (телефонними) лініями зв'язку, припускає контактне

підключення апаратури розвідки до кабелів або дротів. Найпростіший спосіб – це безпосереднє паралельне підключення до лінії зв'язку, але даний факт легко виявляється, оскільки приводить до зміни характеристик лінії зв'язку за рахунок падіння напруги. Тому засоби розвідки до лінії зв'язку підключаються або через погоджучий пристрій, що дещо знижує падіння напруги, або через спеціальні пристрої компенсації падіння напруги. В останньому випадку апаратура розвідки і пристрій компенсації падіння напруги включаються в лінію зв'язку послідовно, що суттєво ускладнює виявлення факту несанкціонованого підключення до неї. Контактний спосіб використовується здебільшого для зняття інформації з коаксіальних і низькочастотних кабелів зв'язку. Електричний канал найчастіше використовується для перехоплення телефонних розмов. При цьому перехоплена інформація може безпосередньо записуватися або передаватися радіоканалом у пункт прийому для її запису й аналізу. Пристрої, що підключаються до телефонних ліній зв'язку з передачею інформації радіоканалоами, називають *телефонним закладенням*.

3. Може використовуватися індуктивний канал перехоплення інформації по каналах телефонного зв'язку, що не вимагає контактного підключення до каналів зв'язку. В даному каналі використовується ефект виникнення навкруги кабелю зв'язку електромагнітного поля при проходженні по ньому інформаційних електричних сигналів, які перехоплюються спеціальними індукційними датчиками. Індукційні датчики використовуються здебільшого для знімання інформації з симетричних високочастотних кабелів. Сигнали з датчиків посилюються, здійснюється частотне розділення каналів, й інформація, що передається окремими каналами, записується на магнітофон. Сучасні індукційні датчики здатні знімати інформацію з кабелів, захищених не тільки ізоляцією, але і подвійною бронею зі сталевої стрічки і сталевого дроту, що щільно обвиває кабель. Для безконтактного знімання інформації з незахищених телефонних ліній зв'язку можуть використовуватися спеціальні низькочастотні підсилювачі, забезпечені магнітними антенами.

Найбільш небезпечні методи знімання комп'ютерної інформації. При цьому основні можливості несанкціонованого доступу забезпечуються шкідливим програмним забезпеченням, що включає комп'ютерні віруси, троянські програми, програмні закладення. Такі програми порушують штатний режим функціонування комп'ютера, даючи зловмиснику можливість дістати доступ до інформації. Це найбільш вразлива сфера витоку інформації.

Робота комп'ютерів, модемів, обладнання корпоративної мережі супроводжується електромагнітними випромінюваннями, які теж є джерелами сигналу, здатного сформувати певні канали витоку інформації. Такими джерелами можуть бути материнські плати комп'ютерів, блоки живлення, плати принтерів, жорсткі диски і тому подібне. Проте, як показує статистика, основним джерелом високочастотного

електромагнітного випромінювання є дисплей, що використовує електронно-променеву трубку.

Перераховані вище методи отримання інформації засновані на використанні технічних (зовнішніх) каналів витоку. Але особливу увагу при розгляданні загроз слід приділити внутрішнім, «людським» каналам витоку інформації. Внутрішні канали витоку пов'язані з адміністрацією й обслуговуючим персоналом, політикою безпеки, ретельною організацією режиму роботи.

Серед них у першу чергу потрібно наголосити на таких каналах витоку, як розкрадання носіїв інформації і несанкціоноване копіювання. Але до найпоширеніших із внутрішніх каналів витоку є ненавмисне розкриття інформації співробітниками унаслідок некомпетентності або недисциплінованості. Незнання правил роботи з конфіденційною інформацією, невміння визначити, які дані є конфіденційними, можуть привести до розсекречення даних. Навмисна видача інформації зустрічається рідше, зате здійснюється цілеспрямовано і з самими небезпечними наслідками для підприємства.

5.4 Аналіз рівня інформаційної безпеки вузла комутації

5.4.1 Аналіз інформаційних об'єктів, що захищаються

Для аналізу рівня інформаційної безпеки (ІБ) вузла комутації необхідно скласти перелік його об'єктів і підсистем, які підлягають захисту, і суб'єктів (людей і організацій), які задіяні в інформаційній мережі і впливають на інформаційний захист. При цьому необхідно стисло описати підсистеми з погляду інформаційної безпеки.

Характеристики об'єктів / інформаційних підсистем вузла комутації включають наступні категорії:

1. Обладнанняя телефонної комутації на базі станції 5ESS.
2. Апаратне забезпечення інформаційної системи (комп'ютери, модеми, принтери, маршрутизатори і кабелі комп'ютерної мережі).
3. Забезпечення мережі змінного струму (силові мережні кабелі, роз'єднувачі, автоматичні реле, розетки).
4. Системне програмне забезпечення (операційні системи, міжмережні екрани, антивірусні програми, програми для корпоративної VPN, програми резервного копіювання).
5. Прикладне програмне забезпечення (офісні програми, інтернет-програми, додаткові програми).
6. Організаційне забезпечення – користувачі інформаційної системи (системні адміністратори, адміністративний персонал, інженери).
7. Нормативне забезпечення (правила внутрішнього розпорядку підприємства, положення про конфіденційну інформацію, посадові обов'язки служби безпеки, системних адміністраторів та інженерів, правила інформаційної безпеки підприємства, інструкції для роботи).

8. Види даних – інформація, яка використовується в роботі системи в її виробничому значенні (дані про абонентів, інформація про канали та трафік, інформація про конфігурацію станції тощо).

Таким чином, має бути складено список інформаційних об’єктів і підсистем вузла комутації, що захищаються.

5.4.2 Формування моделі загроз

Необхідно знати потенційно можливі втрати різної інформації, що підлягає захисту. Витрати на захист не повинні перевищувати можливі збитки при втраті інформації.

Фундаментальні властивості інформації, що захищається, які визначають її цінність – це: конфіденційність, цілісність, доступність та спостережність:

1. Конфіденційність – це властивість інформації, яка полягає в тому, що вона не може бути доступною для ознайомлення користувачам та/або процесам, що не мають на це відповідних повноважень.

2. Цілісність інформації – це властивість, яка полягає в тому, що вона не може бути доступною для модифікації користувачам та/або процесам, що не мають на це відповідних повноважень. Цілісність інформації може бути фізичною та/або логічною.

3. Доступність інформації – це властивість, що полягає у можливості її використовування за першою вимогою користувача, який має відповідні повноваження.

4. Спостережність – це властивість інформації, яка полягає в тому, що процес її оброблення може безперервно перевувати під контролем органу (суб’єкта), що управляє захистом.

Загрози – це шляхи реалізації дій, які є небезпечними. Наприклад, загроза зняття інформації приведе до втрати конфіденційності, загроза пожежі веде до порушення цілісності і доступності інформації, загроза обриву каналу зв’язку може привести до втрати доступності.

Специфічна модель загроз для вузла комутації відповідає вимогам керівного нормативного документа «Типова модель загроз для інформаційних ресурсів цифрових комутаційних систем, які використовуються в мережах електрозв'язку загального користування України» (КНД 45-164-2001).

Загрози можуть здійснюватися через:

– технічні канали (акустичні, оптичні й інші канали витоку);

– канали спеціального впливу (формування полів і сигналів з метою злому системи захисту або порушення цілісності інформації);

– несанкціонований доступ (підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання засобів захисту для використання інформації, вживання заставних пристроїв або заставних програм, використання комп’ютерних вірусів).

Розглянемо об’єкт захисту від загроз НСД – вузол комутації мобільного оператора на базі 5ESS – як інформаційну систему з точки зору ІБ. Потенційними каналами загроз НСД можуть бути наступні елементи:

– АТС (вузол комутації) на базі станції 5ESS, зокрема її термінали;

– зовнішні телефонні канали (з’єднувальні лінії), мідні й оптичні);

– внутрішні телефонні лінії;

– сервери комп’ютерної мережі;

– робочі місця комп’ютерної мережі, термінали інженерів;

– елементи мережного обладнання (маршрутизатори);

– безперебійні блоки живлення;

– системи захисту інформації;

– консолі адміністраторів комп’ютерної мережі;

– засоби документування інформації (принтери);

– засоби завантаження і розповсюдження програмного забезпечення;

– фізичні і віртуальні носії інформації (ПЗП, ОЗУ, стрічки, магнітні, лазерні, магнітооптичні й інші накопичувачі);

– внутрішні кабелі зв’язку (внутрішньо мережні інтерфейси);

– зовнішні канали зв’язку інформаційної системи (вихід в IP-мережі).

Враховуючи, що порушник може використати як штатні, так і інші канали доступу, потрібно визначити основні потенційні канали НСД, через які можуть здійснюватися потенційні загрози шляхом отримання порушником НСД до апаратних, телекомунікаційних і програмних засобів інформаційної системи. Потенційними об’єктами атак порушника в інформаційній системі можуть бути:

1. Штатні апаратні засоби вузла комутації – операційна система та програмне забезпечення станції 5ESS.

2. Штатні апаратні засоби інформаційної системи (при використанні їх користувачами не за призначенням і за межами своїх повноважень).

3. Штатні апаратні засоби корпоративної мережі (при використанні їх сторонніми особами).

4. Технологічні пульти управління – системні термінали, консолі.

5. Лінії зв’язку між апаратними засобами інформаційної системи.

6. Побічні електромагнітні випромінювання і наведення (ПЕМВН) апаратних і телекомунікаційних засобів оброблення і передачі інформації інформаційної системи, побічні наведення інформації в мережі електроживлення і заземлення апаратури системи, побічні наведення інформації по ланцюгах допоміжних та інших сторонніх комунікацій в окремих приміщеннях і на території об’єкта.

7. Відходи обробки інформації у вигляді паперових, магнітних тощо носіїв.

8. Програмне забезпечення інформаційної системи.

9. Можливі потенційні канали несанкціонованого доступу і несанкціонованого впливу.

При розробці моделі загроз з погляду можливого порушення властивостей захищеності інформації розрізняють наступні класи загроз

інформації: порушення конфіденційності; порушення цілісності; порушення доступності (відмова в обслуговуванні); порушення спостережності (керованості).

Загроза – це потенційно можлива несприятлива дія на інформацію, яка приводить до порушень хоча б однієї з чотирьох наведених властивостей.

1. ***Загрози конфіденційності***.

Існують наступні два основні шляхи порушення конфіденційності:

– унаслідок втрати контролю над системою захисту інформації (СЗІ);

– через канали витоку інформації.

Втрата управління СЗІ може бути реалізована внаслідок джерел порушень безпеки. Крім того, джерела порушень безпеки можуть бути причиною виникнення прихованих каналів витоку інформації.

Канал витоку інформації – це спосіб отримання інформації за рахунок використання шляхів передавання інформації, які присутні в інформаційній системі, але не контролюються або не спостерігаються СЗІ. Захист від витоку інформації засновано на виборі правильної політики безпеки, а також на можливостях контролю інформаційних потоків та виведення інформації. Побічні канали витоку з випромінювання, електроживлення або акустики також є тимчасовими каналами. В даному випадку захист досягається за допомогою екранування, зашумлення, фільтрації.

2***. Загрози цілісності.***

Загроза цілісності інформації (загроза її зміни) означає активну дію на інформацію з боку порушника, тобто небезпеку незаконної модифікації інформації. При загрозі цілісності замість звичного каналу витоку слід ввести поняття каналу дії на цілісність, це вимагає доступу на запис. Приклад виникнення каналу дії на цілісність (тобто несанкціонованої зміни) інформації – дія «троянської» програми, яка здійснює явні або приховані активні дії на користь розробника програми – зловмисника.

Порушення цілісності може виникнути внаслідок створення випадкових або навмисних критичних ситуацій, зараження вірусами, програмних закладок і тому подібного. Всі причини і джерела НСД можуть створити порушення цілісності інформації.

Серед механізмів захисту від порушень цілісності виділяються такі:

– введення надлишковості в інформацію (наприклад, вживання циклічного кодування, контрольних сум, що дозволяє контролювати її цілісність);

– своєчасне і регулярне копіювання цінної інформації;

– введення надлишковості в процес оброблення інформації, тобто використовування автентифікації, що дозволяє контролювати цілісність файлів, повідомлень і програм;

– введення системної надлишковості (наприклад, дублювання даних).

3. ***Загрози доступності***.

Суб'єкт інформаційної системи, використовуючи її ресурси, за правилами політики безпеки, повинен отримати інформацію в необхідному йому вигляді, місці і своєчасно.

Властивість доступності забезпечується правильним використанням ресурсів, стійкістю до відмов, їх ефективної заміни компонентів інформаційної системи та їх резервування, здатністю до швидкого відновлення після збоїв.

У більшості випадків доступність інформації в інформаційній системі визначається працездатністю самої системи, а основна загроза доступності – втрата продуктивності. Заходи для підтримки працездатності системи:

– підтримка всіх користувачів (інженерів вузла);

– підтримка програмного забезпечення і контроль за ним;

– управління і зміна конфігурацій мережного обладнання, комп'ютерів;

– резервне копіювання даних, настройок, системного і прикладного ПЗ;

– управління носіями інформації, що забезпечує фізичний захист носіїв: жорстких дисків, магнітних стрічок, оптичних дисків, немагнітних накопичувачів;

– документування процедур;

– збір і аналіз лог-файлів (журналів реєстрації подій);

– регламентні роботи.

Результат загрози доступності – відсутність доступності інформації або відсутність каналів доступу до інформації.

4. ***Загрози спостережності***.

Спостережність формує канали нагляду за інформацією. Канали нагляду – це канали, через які можливе читання («нагляд») інформаційних процесів і об'єктів. Загрози спостережності полягають в тому, що у користувача відсутня можливість спостерігати за об'єктами системи. Іншими словами, загрози спостережності до порушення каналів нагляду, а головна задача спостережності в інформаційній системі – це підтримка функціонування каналів нагляду. Задача спостережності реалізується за допомогою наступного:

– реєстрація подій (аудит);

– ідентифікація й автентифікація користувачів і ресурсів;

– достовірний канал;

– розподіл обов'язків;

– цілісність комплексу засобів захисту (КСЗІ);

– самотестування;

– автентифікація обміну, відправника й отримувача.

Спостережність зводиться до протоколювання (лог-файлів) і аудиту. *Протоколювання* – це збірання й накопичення інформації про події, які відбуваються у системі. *Аудит* – це аналіз інформації про події.

Протоколювання й аудит організовуються для наступних цілей:

– забезпечення звітності користувачів та адміністраторів;
– забезпечення можливості розбору послідовності подій;
– виявлення спроб порушення інформаційної безпеки (ІБ);
– пошук і надання інформації для виявлення й аналізу проблем ІБ.

5.4.3 Формування моделі порушника

Порушник – суб'єкт, який зробив спробу виконання заборонених дій помилково, по незнанню або усвідомлено зі злим наміром або без такого, і який використовує для цього різні методи і засоби.

Абстрактний опис порушника («модель порушника») дає основу для опису необхідних параметрів КСЗІ та вимог до захисту від несанкціонованого доступу до інформаційної системи.

Розробка моделі порушника полягає в переліку й аналізі його елементарних цілей. Крім того, потрібно описати способи досягнення цілей порушника, що дасть список потенційно можливих атак на інформаційну систему вузла комутації, що захищається. При цьому реальні цілі порушника і механізми здійснення атак будуть виражатися комбінаціями його елементарних цілей і видів атак.

Таким чином, побудова моделі порушника полягає у складанні й описі множини елементарних атак на інформаційну безпеку.

Модель порушника дає:

– категорії (типи) порушників, які здатні проводити атаки;

– цілі, які можуть переслідувати порушники, і засоби, що ними використовуються;

– сценарії атак порушників і способи їх дій на кожному етапі атак.

Сценарій імовірних атак (дій) порушників показують види акцій (дій), що скоєні порушниками, а також способів дії на кожному етапі.

Слід враховувати як зовнішніх порушників, що проникають на територію, в приміщення або інформаційну мережу вузла комутації ззовні, так і внутрішніх, тобто зловмисників з числа інженерів вузла або з числа відвідувачів, що мають допуск до приміщення вузла. Можлива змова і сумісні дії зовнішніх і внутрішніх порушників.

Слід звернути увагу на необхідність визначення зон, на які можуть бути спрямовані цілі порушника. До них відносяться зони доступу до особливо цінних документів, матеріалів, обладнання, носіїв інформації, а також зони можливого вживання диверсійних засобів.

При пасивному перехопленні порушник лише стежить за повідомленнями, які передаються, без втручання в їх потік, що дає йому можливість розкрити зміст повідомлення. Крім того, порушник може також стежити за заголовками повідомлень (навіть якщо дані в повідомленні йому незрозумілі) з метою отримання ідентифікаторів процесів, які беруть участь у передачі даних. Він може аналізувати трафік – узнати службову інформацію, довжину повідомлень, їх кількість і щільність.

При активному перехопленні порушник виконує несанкціоновані дії (НСД) над повідомленнями, які передаються. За такогоу виду перехоплення повідомлення можуть бути вибірково змінені, знищені або затримані, а також він може створювати фальшиві повідомлення.

Необхідно розглядати і дії порушника, який отримав НСД, і помилки програмного забезпечення, й вразливості мережних протоколів.

Існують основні категорії загроз на вузлі телефонної комутації:

– розкриття змісту передаваних повідомлень;

– аналіз трафіка (можливість визначити ідентифікатори відправника й отримувача даних, кількість і розмір повідомлень);

– зміна потоку повідомлень (порушення режиму роботи об’єкта);

– несанкціоноване встановлення з’єднання;

– відмова в наданні послуг (інформації).

Отже, модель типових варіантів зловмисної поведінки порушника така:

1. Отримати несанкціонований доступ до інформації, яка підлягає захисту.
2. Видати себе за іншого користувача, щоб використати його повноваження з метою формування помилкової інформації, зміни інформації.
3. Відмовитися від факту формування переданої інформації (наприклад, знищивши сліди своїх дій).
4. Стверджувати, що інформація отримана від санкціонованого користувача, хоча вона сформована самим порушником.
5. Стверджувати, що отримувачу у встановлений термін було передано інформацію, яка насправді не передавалася або передавалася в інший час.
6. Відмовитися від факту отримання інформації або стверджувати про інший час її отримання.
7. Несанкціоновано змінити повноваження інших санкціонованих користувачів – розширити або обмежити повноваження, видалити або додати обліковий запис.
8. Несанкціоновано розширити свої повноваження доступу до інформації.
9. Приховати факт наявності деякої інформації в іншій інформації.
10. Підключитися до ліній зв’язку між іншими користувачами.
11. Узнати, хто і до якої інформації має доступ («аналіз трафіка»).
12. Модифікувати програмне забезпечення (вилучення функцій або вставка нових функцій).
13. Змінити протокол обміну інформацією з метою його порушення.
14. Заважати обміну повідомленнями шляхом введення перешкод з метою порушення автентифікації повідомлень.

Перераховані вище варіанти алгоритмів поведінки порушника в інформаційних мережах говорять про те, що важливо знати, кого вважати порушником, і розробити модель його можливої поведінки. При цьому в

ролі потенційного порушника може бути не лише стороння особа, але і системний адміністратор, який спроможний приховати свої дії.

Аналіз списку загроз свідчить про те, що захист від них доцільно концептуально розділити на два рівні:

– захист від користувачів;

– захист від загроз дій потенційними каналами несанкціонованого доступу до елементів інформаційної мережі.

Виділяють наступні шляхи проникнення у систему, порушення працездатності СЗІ або несанкціонованого доступу до інформації:

– фізичне руйнування системи або виведення окремих найважливіших компонентів або інформаційної системи з ладу;

– відключення або виведення з ладу допоміжних підсистем системи (електроживлення, вентиляція, лінії зв’язку і тому подібне);

– дії з дезорганізації функціонування системи (зміна режимів робіт пристрою або програм, постановка активних радіоперешкод);

– запровадження агентів до числа працівників системи;

– вербування (через підкуп, шантаж) працівників чи користувачів;

– вживання підслуховуючих пристроїв, дистанційна зйомка;

– перехоплення ПЕМВ, акустичних й інших випромінювань, а також наведень активних випромінювань на допоміжні технічні засоби (телефонні лінії, мережі живлення, водопостачання, опалювання тощо);

– перехоплення даних, переданих каналами зв’язку, їх аналіз з метою з’ясування протоколів обміну, правил входу в зв’язок й авторизації користувача й подальших спроб їх імітації для проникнення у систему;

– розкрадання носіїв інформації (магнітних і оптичних носіїв);

– несанкціоноване копіювання носіїв інформації;

– розкрадання відходів (паперів, матеріальних носіїв інформації);

– читання не стертої інформації із зовнішніх пристроїв пам’яті;

– незаконне отримання паролів й інших даних про розмежування доступу з наступним маскуванням від зареєстрованого користувача;

– несанкціоноване використання терміналів користувачів/інженерів;

– розкриття інформаційного криптозахисту;

– впровадження апаратних закладок, «вірусів», «троянських програм»;

– незаконне підключення до ліній зв'язку з метою підміни законного користувача шляхом його відключення після успішної автентифікації.

Зловмисник звичайно використовує сукупність з перерахованих вище шляхів у вигляді, застосовуючи наступні напрями злочинних дій:

– крадіжка носіїв інформації;

– крадіжка документів;

– зловмисні дії користувача або програми;

– несанкціонований віддалений доступ;

– помилки в роботі користувачів або програмного технічного засобу;

– несанкціоноване використання ліній зв’язку («перехоплення»);

– неправильна робота ліній зв’язку («підробка»).

Оскільки на вузлі телефонної комутації використовуються різні інформаційні технології, то модель порушника повинна бути адекватна реальному порушнику.

Для формування моделі порушника розробимо припущення: про категорію осіб, до яких може належати порушник;

– про кваліфікацію порушника та його технічну оснащеність, про методи і технічні засоби, що використовуються;

– про мотиви дій порушника;

– про характер можливих дій порушника.

Порушник – це особа, яка зробила спробу виконання заборонених дій і використовує для цього різні методи і засоби. Можливі типи порушників інформаційної безпеки вузла:

1) «Недосвідчений або неуважний користувач» – інженер вузла комутації, який може робити спроби виконання заборонених операцій, доступу до недоступних йому захищених ресурсів системи, введення некоректних даних і тому подібного; його дії помилкові через некомпетентність або халатність (без злого наміру), і він використовує при цьому лише доступні йому штатні апаратні і програмні засоби.

2) «Любитель» – інженер, який намагається подолати систему захисту без корисливих цілей, а з метою самоствердження. Для подолання системи захисту та здійснення заборонених дій він може використовувати різні методи отримання додаткових повноважень доступу до ресурсів (імен, паролів), недоліки в побудові системи захисту і доступне йому штатне програмне забезпечення (ПЗ); його несанкціоновані дії засновані на перевищенні своїх повноважень і використанні дозволених засобів, крім цього він може намагатися використовувати додатково нештатне ПЗ (наладчики, службове ПЗ, сніфери тощо) або додаткові засоби.

3. «Зовнішній порушник/зловмисник» – стороння особа, яка діє цілеспрямовано з корисливих інтересів або з цікавості, можливо в змові з іншими особами. Він може використовувати весь набір методів і засобів злому систем захисту, характерних для мереж на основі IP-протокола, включаючи дистанційне упровадження програмних закладок і вживання спеціальних інструментальних і технологічних програм, використовуючи наявні слабкості в системі захисту інформації.

4. «Внутрішній зловмисник» – інженер, який діє цілеспрямовано з корисливих інтересів або помсти, можливо в змові із співробітниками або сторонніми особами. Він може використовувати весь набір методів і засобів злому системи захисту, включаючи агентурні методи отримання даних доступу (імен/паролів), пасивні засоби (технічні засоби перехоплення без модифікації), методи і засоби активної дії (модифікація інформації, підключення до каналів передачі даних, запровадження програмних закладок і використання спеціальних програм), а також комбінації дій як зсередини, так і ззовні – з IP-мереж загального користування.

Порушник може належати до наступних категорій персоналу:

– зареєстровані користувачі системи (інженер підприємства);

– персонал, обслуговуючий інформаційну систему (адміністратор);

– технічний персонал, обслуговуючий приміщення (співробітники, які мають доступ до будівлі і приміщення, де розташовані компоненти системи);

– служба безпеки;

– керівники.

Сторонні особи, які можуть бути порушниками, це:

– клієнти (абоненти) і партнери (представники організацій, громадяни);

– відвідувачі (запрошені з будь-якого приводу) представники конкуруючих організацій або особи, які діють за їх завданням;

– працівники допоміжних організацій, які взаємодіють з підприємством з питань забезпечення її життєдіяльності (енерго-, водо-, теплопостачання);

– люди, які випадково або навмисно проникли в мережу підприємства з боку зовнішніх телекомунікаційних та IP-мереж.

Приймаються наступні обмеження та припущення щодо характеру дій можливих порушників:

– робота по підбору співробітників підприємства і спеціальні кадрові заходи повинні виключати можливість створення об'єднання порушників, тобто змов та цілеспрямованих дій з подолання системи захисту інформації двох і більш порушників-співробітників;

– порушник приховує свої несанкціоновані дії, зокрема від інших співробітників підприємства;

– несанкціоновані дії можуть бути наслідком помилок користувачів, системних адміністраторів, служби безпеки й охорони, експлуатуючого і обслуговуючого персоналу, а також недоліків інформаційних технологій (табл. 5.1).

Таблиця 5.1 – Категорії порушників та рівень загроз

Категорії потенційних порушників

Категорія порушника	**Рівень загрози**
Технічний персонал, що обслуговує приміщення (співробітники, які мають доступ до приміщень, де розташовані компоненти інформаційної системи)	1
Зареєстровані користувачі системи – інженери	2
Співробітники служби безпеки	3
Керівники різних рівнів	4
Персонал, що обслуговує інформаційну систему (адміністратори)	5

Продовження таблиці 5.1

Специфікація порушника за мотивами порушень

Мотив порушення	Рівень загрози
Безвідповідальність, халатність, некомпетентність	1
Самоствердження	2
Користь, помста	3
Професійна розвідка	4

Специфікація порушника за рівнем кваліфікації

Кваліфікаційні ознаки	Рівень загрози
Формування інформаційних ресурсів	1
Високий рівень знань і досвід роботи із засобами обробки інформації	2
Високий рівень знань програмного забезпечення та побудови інформаційної системи	2
Знання структури, функцій і механізмів дії системи захисту інформації, а також їх недоліків	3
Знання недоліків та вразливостей програмного забезпечення системи захисту інформації, а також не документованих можливостей	3
Розробник системного програмного забезпечення (ПЗ), системи захисту інформації або шкідливого ПЗ	4

Специфікація порушника за можливістю використання різних засобів

Характеристика можливих засобів	Рівень загрози
Агентурні методи отримання відомостей	1
Пасивні засоби знімання інформації	2
Штатні засоби та недоліки КСЗІ, знімні носії	2
Методи дистанційного впровадження закладок, блокування роботи, знімання інформації	3
Методи активного впливу (модифікації)	4

Специфікація порушника за тривалістю дії

Характеристика часових можливостей	Рівень загрози
До впровадження інформаційної системи	1
При непрацюючій системі захисту інформації (під час перерв, переривання обслуговування і так далі)	2
Під час функціонування інформаційної системи	3
Доступ до системи без обмеження в часі	4

Специфікація порушника за місцем дій

Характеристика місця дії	Рівень загрози
Без доступу на контрольовану територію	1
З контрольованої території, але без доступу до приміщення інформаційної системи	1
У приміщеннях інформаційної системи, але без прав доступу до засобів роботи з інформацією	2
З робочого місця користувача	3
З доступом до бази даних, документів, архівів	3
З доступом до управління засобами захисту	4

Важливо мати на увазі, що витрати на систему захисту інформації від несанкціонованого доступу необхідно зіставляти та приводити у відповідність з цінністю інформації й інших інформаційних ресурсів, які підлягають захисту, а також зі збитками, які можуть бути нанесені внаслідок несанкціонованого доступу.

Для оцінки захищеності необхідно враховувати наступні чинники:

– збитки, які може нанести порушення захищеності інформації з урахуванням можливих наслідків порушення конфіденційності, цілісності і доступності інформації;

– реальна ймовірність порушення захисту інформації з обмеженим доступом з урахуванням захищеності і засобів контролю.

Отже, наступний крок створення КСЗІ – це складання проекту захисних заходів щодо кожного з виявлених видів загроз, застосовуючи штатні та додаткові засоби захисту.

5.5 Штатні засоби захисту станції 5ESS

Система комутації 5ESS забезпечена вбудованими можливостями по захисту інформації, основними з яких є: контроль цілісності програмного забезпечення, ідентифікація й автентифікація користувачів (ім’я/пароль), розподіл прав доступу (повноважень) за персональними та термінальними принципами, реєстрація всіх команд, звітів і змін в базі даних. Розглянемо кожен із засобів захисту інформації на 5ESS детальніше.

1. Контроль цілісності програмного забезпечення (ПЗ) забезпечується на всіх етапах. Файли системного та прикладного ПЗ перевіряються за контрольними сумами. Спеціальні підпрограми (audit) перевіряють наявність невідповідність у програмах або даних; якщо будуть знайдені помилки, то вірні файли будуть узяті з дубльованого блока, або з блока вищої ієрархії, або з жорсткого диска станції, в крайньому випадку – з первинної завантажувальної стрічки. Програми різних audit-застосувань запускаються як автоматично за розкладом, так і у разі підозри на помилку в програмі або даних. Верхній рівень audit-программ – рівень ядра ОС UNIX-RTR – перевіряється підпрограмою System Integrity Monitor (SIM). Крім цього, audit-програми перевіряють центральний процесор, файлову систему, менеджер пам’яті, базу даних обладнання, буфер повідомлень, ініціалізацію процесів.

2. Ідентифікація й автентифікація користувачів в 5ESS також надійна як і в будь-якій unix-подібній операційній системі. За будь-якого входження в 5ESS користувач повинен відкрити діалог у терміналі й ввести свої ім.’я (user name) і пароль (password). Перший пароль користувачу дає так званий «супер-користувач», тобто інженер станції, що відповідає за СЗІ і розподіл повноважень (прав); при першому входженні станція 5ESS просить змінити пароль, після чого він відомий лише самому користувачу (інженеру) станції. Пароль зберігається у файловій системі 5ESS у зашифрованому виді, і при його втраті немає ніякої можливості увійти до термінала 5ESS або змінити пароль. Для надійної автентифікації

довжина пароля повинна бути великою, не менше 7 символів, і містити літери латиниці, цифри і знаки.

Для захисту від злому (підборання) пароля число спроб (помилок) введення пароля обмежено, після чого термінал закриває діалог, і його ім’я (tty name) видається у звіті про спробу несанкціонованого доступу.

Крім того, для надійнішого захисту пароля в 5ESS настроюється «час життя» пароля, після якого користувач повинен змінити пароль. Якщо він не змінить пароль, то його доступ в станцію блокується до зміни пароля.

Більше того, зберігається історія паролів, так що три останні паролі користувача не можуть повторюватися.

3. Розподіл прав доступу («управління повноваженнями») користувачів (інженерів) за персональними і термінальними принципами засновано на їх ідентифікації й автентифікації. Користувач, що увійшов до термінала станції 5ESS може вводити різні команди (з експлуатації і техобслуговування станції, вимірювання трафіка тощо). Всі команди 5ESS поділені на групи (command group). Кожна група відповідає, по-перше, типу об’єкта (канали, абоненти, стан обладнання, система, БД і так далі); по-друге, типу дії (читання або створення/змінення/видалення). Дані класи команд «супер-користувач (інженер, що відповідає за розподіл повноважень)», тобто адміністратор, призначає кожному користувачу (user name) і кожному терміналу (tty name). Лише у випадку, якщо команда, яку намагається виконати користувач (інженер 5ESS), дозволена і йому, і терміналу, з якого він її ввів, команда буде поставлена в чергу на виконання, і всі результати з її виконання («звіт» – report) будуть видані і на даний термінал (tty), і на загальностанційний термінал-«принтер» для всіх звітів (rop = receive only printer).

Для зручності управління персональними (user) і термінальними (tty) повноваженнями на станції 5ESS існують так звані «профілі команд» (command group profile), які інженер, що відповідає за розподіл повноважень, може створювати на свій розсуд, вносячи в їх бажані набори командних груп (command group). Тоді при створенні нового користувача – інженера станції 5ESS – замість призначення великого числа класів команд буде достатньо призначити йому відповідні «командні профілі», наприклад такі, як: лише переглядання обладнання або БД, або зміни стану обладнання, або зміни БД, або для управління системою, або техобслуговування, або для обліку трафіка і так далі в будь-якій комбінації профілів.

4. Реєстрація всіх команд і змін БД в лог-файлах («журналах», реєстраційних файлах) – це важливий засіб протоколювання всіх дій користувачів (інженерів). В станції 5ESS існує велика кількість (декілька десятків) лог-файлів, два з яких містять команди користувачів:

– CMDLOG – лог-файл команд («command log»), яка містить усі команди, введені в станцію; крім команди і її параметрів вказано номер діалогу та ім’я користувача (user id);

– ORIGLOG – лог-файл модифікацій БД ODD (Office-Dependent Database), яка містить інформацію про будь-які додавання, зміни і видалення записів у БД ODD; при вставленні або зміні запису файл містить поточний запис (параметри і значення), при видаленні запису з ODD цей лог-файл містить оригінальний, первинний запис (тому і називається 'original log').

Реєстрація всіх звітів станції 5ESS теж проводиться в різні лог-файли, що дозволяє мати інформацію для відновлення послідовності подій у разі потреби аналізу ситуації, пов'язаної із захистом інформації. Всі звіти розбиті на класи (message classes), що допомагає збирати й аналізувати інформацію про події.

Набір вищеперелічених штатних засобів системи комутації 5ESS достатньо для створення КСЗІ на вузлі комутації мобільного оператора, побудованого на базі станції 5ESS.

5.6 Вибір заходів захисту інформації на вузлі комутації

Заходи і методи захисту інформації наступні: перешкоди, управління доступом, маскування, регламентація і спонукання.

Перешкода – це фізичне перегороджування шляху зловмиснику до інформації, що захищається (до апаратури, носіїв інформації тощо).

Управління доступом – це захист інформації шляхом регулювання повноважень на використання кожного з ресурсів інформаційної мережі. Управління доступом включає наступні функції захисту: ідентифікація користувачів і ресурсів (привласнення кожному об'єкту персонального ідентифікатора); автентифікація об'єкта або суб'єкта за ідентифікатором; перевірка повноважень; дозвіл роботи в межах установленого регламенту; реєстрація звернень до ресурсів, що захищаються; реагування (сигналізація або відмова) при спробах несанкціонованих дій.

Маскування – це захист інформації в інформаційній системі шляхом її криптографічного перетворення, тобто «приховування інформації».

Регламентація – це захист інформації шляхом створення процедур і правил оброблення, зберігання та передавання інформації, за яких можливість несанкціонованого доступу зводилася б до мінімуму.

Спонукання (примушення) – це захист інформації шляхом спонукання користувачів системи не порушувати установлений регламент (правила).

Ці методи захисту інформації реалізуються такими основними засобами: фізичними, апаратними, програмними, криптографічними, організаційними, законодавчими (нормативними) і морально-етичними.

Фізичні засоби захисту призначені для охорони території об'єктів, захисту компонентів інформаційної системи вузла комутації. Це механічні засоби, електронна система охорони приміщень, організація пропускного режиму та нагляду, пожежна сигналізація та запобігання розкраданню носіїв інформації й іншого майна. Крім того, для організації охорони обладнання інформаційної системи підприємства та носіїв інформації

(стрічки, диски, зовнішня пам’ять) використовуються спеціальні сейфи і металеві шафи для установки в них окремих елементів інформаційної системи (сервери, маршрутизатори) та переміщуваних носіїв інформації.

Апаратні засоби захисту – електронні й електромеханічні пристрої внутрішнього захисту елементів, засобів і систем (комп’ютерів, обладнанання, ліній зв’язку тощо). Апаратні засоби забороняють НСД віддаленого користувача (зловмисника) до інформаційної системи, а також внутрішній доступ до окремих елементів інформаційної системи, можливий в результаті випадкових або навмисних дій співробітників.

Програмні засоби захисту виконують логічні функції захисту і входять як до складу програмного забезпечення інформаційної системи, так і до складу системи захисту інформації. Програмні засоби найбільш поширені, завдяки їх універсальності, гнучкості, простоті реалізації, можливості зміни, але вони є найвразливішими елементами захисту:

1) Захист інформації від витоку акустичними каналами – це комплекс заходів, що виключають або зменшують можливість виходу конфіденційної інформації за межі контрольованої зони підприємства за рахунок акустичних полів.

Основними заходами в цьому виді захисту виступають організаційні та технічні заходи. Організаційні заходи – це проведення просторових і режимних заходів, а технічні – це пасивні (звукопоглинання, звукоізоляція) й активні (звукоглушіння) заходи. Режимні заходи передбачають суворий контроль перебування в контрольованій зоні співробітників та відвідувачів. Технічні заходи передбачають використання звукопоглинальних засобів. Пористі та м’які матеріали (пінобетон, пориста штукатурка і так далі) є хорошими звукоізолюючими і звукопоглинальними матеріалами.

Активні засоби – це генератори шуму, що виробляють шумоподібні акустичні сигнали. Вони використовуються в спеціальних приміщеннях, що вимагають особливого захисту. Акустичні датчики цих генераторів шуму створюють акустичний шум у приміщенні, а вібраційні – маскуючий шум у захисних конструкціях.

2) Захист інформації від витоку електромагнітними каналами – це заходи, що виключають або послаблюють можливість виходу конфіденційної інформації за межі контрольованої зони за рахунок електромагнітних полів і наведень побічного характеру.

Інженерно-технологічні заходи щодо запобігання каналам витоку інформації за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН) в технічних засобах наступні:

– екранування елементів і вузлів апаратури, зокрема обладнання АТС 5ESS, серверів, комп’ютерів, принтерів, обладнання локальної мережі, обладнання живлення, кондиціонування і так далі;

– послаблення електромагнітного, ємнісного, індуктивного зв’язку між елементами і струмонесучими дротами;

– фільтрація сигналів у ланцюгах живлення та заземлення, використання обмежувачів, розв'язуючих ланцюгів, систем взаємної компенсації, послаблювачів з ослаблення або знищення ПЕМВН.

Електростатичне екранування полягає в замиканні силових ліній електростатичного поля джерела на поверхню екрана і відведенні наведених зарядів на масу та на землю. Таке екранування усуває паразитні зв'язки ємностей. Магніто-статичне екранування засновано на замиканні силових ліній магнітного поля джерела в товщі екрана, що має малий магнітний опір для постійного струму в області низьких частот.

Електромагнітне екранування застосовується при високій частоті сигналу. Дія електромагнітного екрана заснована на тому, що високочастотне електромагнітне поле послабляється ним же створеним полем зворотного напряму, завдяки вихровим струмам, що утворюються в товщі екранау. Заземлення та металізація апаратури надійно відводять наведені сигнали на «землю» та послабляють паразитні зв'язки та наведення між ланцюгами.

Необхідно встановити фільтри в ланцюги живлення постійного та змінного струму, які приглушують або послабляють шкідливі сигнали при їх виникненні або розповсюдженні, а також захищають системи живлення.

Організаційні заходи орієнтовані на вибір місць установки технічних засобів з урахуванням особливостей їх електромагнітних полів з таким розрахунком, щоб виключити їх вихід за межі контрольованої зони.

Крім того, необхідно здійснити екранування приміщень, в яких знаходяться засоби з великим рівнем побічних електромагнітних випромінювань, – приміщення обладнання АТС, приміщення для цифрових систем передачі (ЦСП), серверна, центр управління станцією МСС (Master Control Center). Екранування здійснюється шляхом покриття стін, підлоги та стелі дротяними сітками або фольгою. Для захисту вікон застосовують металізовані штори. Всі екрани потрібно з'єднати з шиною заземлення. Для захисту від наведень на електричні ланцюги вузлів і блоків інформаційної системи для монтажу використовують екранований кабель, екрановані роз'єднувачі, мережні фільтри приглушення електромагнітних випромінювань.

3) Захист інформації від витоку матеріальними каналами – це комплекс заходів, що виключають або зменшують можливість неконтрольованого виходу конфіденційної інформації за межі контрольованої зони у вигляді виробничих відходів (фрагментів документів, чернеток, зіпсованих роздруківок і тому подібного). Організаційними заходами захисту є використання знищувачів паперу й очищення пам'яті (наприклад, форматування) при виносі носіїв інформації за межі охоронного периметра вузла. Таким способом повинні бути перероблені знищувані архівні документи (зі складанням спеціального акту).

4) Захист інформації підприємства від витоку телефонними каналами актуальний для фізичних (мідних) кабелів. Він полягає в контролі

дротяних телефонних ліній на предмет виявлення в них інформаційних сигналів і вимірюванні параметрів цих ліній.

Методи контролю телефонних ліній засновані на тому, що будь-яке підключення до них викликає зміну електричних параметрів ліній: амплітуд напруги та струму в лінії, а також значень ємності, індуктивності, активного та реактивного опору лінії.

Найвразливішими місцями підключення є: розподільний щит, внутрішні розподільні колодки та відкриті ділянки дротів, телефонні розетки й апарати. Найефективніший спосіб виявлення засобів знімання інформації, що підключаються до телефонної лінії, – це використання локаторів дротяних ліній. При вживанні нелінійного локатора для перевірки телефонної лінії необхідно її роз'єднати та відключити від неї телефонний апарат, підключивши замість нього еквівалентне навантаження; роз'єднання (відключення телефонної лінії) доцільно проводити на ввідній розподільній коробці (щитку) будівлі, підключення локатора до лінії здійснюється в місці її роз'єднання. При використанні локатора телефонних ліній можливе визначення і дальності до місця підключення заставного пристрою з помилкою 2...5 м, що значно полегшує його візуальний пошук.

Для виключення дії високочастотного сигналу на апаратуру АТС в лінію, що йде в її бік, встановлюється спеціальний високочастотний фільтр. Крім того, для захисту інформації вузла комутації від витоку телефонними лініями потрібно застосовувати такі організаційні заходи:

– встановлення контрольованої зони навкруги телефонних кабелів;

– організація контролю й обмеження доступу до приміщень, де проходять телефонні лінії працівників.

5) Захист за допомогою програмних засобів вирішує наступні задачі інформаційної безпеки вузла комутації:

– контроль входу у систему за допомогою ідентифікаторів;

– розмежування та контроль доступу суб'єктів до ресурсів системи;

– ізоляція програм конкретного користувача від інших і від системних ресурсів, тобто забезпечення роботи кожного інженера в індивідуальному середовищі;

– захист інформації від комп'терних вірусів і троянських програм;

– захист конфіденційності інформації шляхом шифрування;

– забезпечення цілісності інформації шляхом введення надлишковості даних;

– резервне копіювання даних;

– автоматичний контроль над роботою користувачів системи на основі результатів реєстрації подій в журналах і підготовка звітів.

Захищена операційна система дає стабільність програмних засобів комплексної СЗІ. Тому на серверах підприємства слід встановити ASP Linux версії «ASPLinux Server V», яка є надійною, високопродуктивною та захищеною платформою. Вона підтримує різну серверну архітектуру, включаючи багатопроцесорні, і системи з великими об'ємами пам'яті.

Вона містить файловий сервер, VPN-сервер (віртуальна приватна мережа) з підтримкою шифрування та стиснення. Фільтр пакетів підтримує фільтри протоколів і засоби обмеження трафікау, може відстежувати трафік за якістю (QoS). Крім стандартних серверних служб ASPLinux Server V включає програмне забезпечення для захисту від спаму та вірусів, управління трафіком, моніторингу і настроювання безпеки.

На робочих комп'ютерах і ноутбуках встановлюється операційна система Windows XP SP2, в якій присутній контроль над дотриманням політики безпеки. Вона задовольняє вимогам криптографічного захисту, тобто може застосовуватися для захисту конфіденційної інформації від потенційного зловмисника, що не є зареєстрованим користувачем.

ASP Linux містить вбудований firewall (міжмережевий екран), який називається iptables. Він займається обробкою мережного трафіка, що проходить через сервер і здійснює фільтрацію паразитного, сміттєвого трафіка (характерного, наприклад, для DdoS-атаки).

Для персональних комп'ютерів і ноутбуків з Windows використовується Outpost Firewall, який захищає від проникнення на комп'ютер. Він блокує спроби віддаленого несанкціонованого доступу і захищає від крадіжки даних, атак типу «відмова від обслуговування» (DoS), порушення конфіденційності, «троянів», шпигунських програм. Outpost Firewall захищає мережні з'єднання, забезпечує локальну безпеку всередині корпоративної мережі, блокує невідомі загрози. Крім того, він запобігає спробам шкідливого коду отримати доступ до системи.

Як антивірусна система для Linux-серверів застосовується calmav, а для Windows-комп'ютерів – Eset NOD32 Antivirus System. Calm AntiVirus інтегровано з серверами електронної пошти для перевірки файлів у повідомленнях. В пакет входить багатопотоковий демон clamd, сканер clamscan, а також модуль оновлення сигнатур freshclam.

Для захищеної роботи віддалених співробітників з корпоративною мережею піприємства використовується технологія VPN – так звана віртуальна приватна мережа. Співробітники встановлюють у себе на віддалених комп'ютерах клієнтську частину VPN під ОС Windows XP, а на сервері під управлінням ASP Linux запускається VPN-сервер з протоколом «Point to Point Tunneling Protocol» на базі пакетау openvpn.

Резервне копіювання є важливою складовою програмних засобів захисту. Для виконання резервного копіювання на комп'ютерах з ОС Windows встановлюється система резервного копіювання та відновлення даних Acronis, що забезпечує дуже швидке відновлення файлів за будь-яких збоїв і об'ємів резервних даних. Acronis True Image створює повні резервні копії комп'ютера та резервні копії найважливіших файлів і даних. Acronis True Image Enterprise Server централізовано дистанційно управляє процесами резервного копіювання та відновлення даних. Acronis Privacy Expert Suite забезпечує попереджуючий захист комп'ютера від шкідливого програмного забезпечення: програм-шпигунів, системних «руткітів» тощо. Для виконання резервного копіювання на Linux-серверах використовується

програма rsync, яка виконує синхронізацію файлів і каталогів, використовуючи кодування даних.

Як офісний пакет використовуються Open Office, який дозволяє звести до мінімуму вразливості при роботі з документами, що містять скрипти.

Як веб-оглядач використовується Firefox 2, який більш захищений ніж Internet Explorer і більш сумісний із www-стандартами. Безкоштовний email-клієнт Mozilla Thunderbird – вільно поширювана поштова програма для роботи з електронною поштою і підтримує протоколи: SMTP, POP3, IMAP і RSS, спам-фильтри й автоматично видаляє рекламу з листів.

Захист документальної інформації – файлів і паперових документів – грунтується на політиці інформаційної безпеки. Обмеження доступу при обробленні електронних і паперових документів, а також ведення їх обліку визначає керівник вузла комутації спільно зі службою безпеки та системним адміністратором. Гриф обмеження доступу та пов'язані з ним захисні засоби повинні враховувати необхідність у використанні інформації або обмеженні доступу до неї, а також збитків, пов'язаних з несанкціонованим доступом або пошкодженням інформації. Слід уникати надавання документам невиправданого грифа обмеження доступу, оскільки це приведе до зниження ефективності використання таких електронних і паперових документів.

Потрібно обраховувати необхідні ресурси для забезпечення захисту інформації з обмеженим доступом:

– створення структури (служби безпеки) для забезпечення захисту інформації з обмеженим доступом, підготовку та підвищення кваліфікації працівників безпеки;

– організацію фізичної охорони, пропускного режиму й охорони приміщень та зберігання матеріальних носіїв інформації з обмеженим доступом;

– розробку внутрішніх документів (інструкцій, правил і положень), які регламентують процес роботи з конфіденційною інформацією;

– забезпечення необхідним обладнанням інженерів підприємства для виконання задач з захисту інформації.

5.7 Планування заходів захисту інформації на вузлі комутації

Заходи щодо безпеки інформаційних ресурсів вузла телефонної комутації мають свої особливості порівнянно з інформаційною безпекою інших систем. Система захисту інформації на вузлі комутації розглядає інформацію, технології її оброблення, користувачів, які використовують ці технології, та визначає інформаційні ресурси, які потребують захисту та вимоги до системи захисту.

Комплексна система захисту інформації (КСЗІ) у застосуванні до захисту вузла комутації складається з двох основних складових:

– використання апаратних і програмних засобів і механізмів штатної системи захисту системи комутації 5ESS;

– запровадження організаційно-технічних заходів, які забезпечують нормальне функціонування комплексу фізичного захисту і механізмів захисту вузла комутації.

КСЗІ вузла комутації на базі станції 5ESS повинна підтримувати множину правил і розмежувань, що регламентують порядок забезпечення захищеності інформаційних ресурсів вузла комутації за допомогою організаційних й інженерно-технічних заходів захисту інформації.

В основу безпеки інформаційних ресурсів вузла комутації покладено адміністративний принцип розмежування доступу з використанням технічних і програмних засобів розмежування доступу згідно з принципом мінімуму повноважень. Для втілення принципу мінімуму повноважень розроблено відповідні нормативно приписуючі інструкції, які регламентують діяльність інженерів вузла комутації.

Дані заходи можуть бути реалізовані шляхом створення КСЗІ на основі штатної системи захисту комутаційної системи 5ESS, на яку отримана експертна оцінка (сертифікат) у Департаменті спеціальних телекомунікаційних систем і захисту інформації (ДСТСЗІ) Служби безпеки України від 23.01.2003 р. № 37.

Структура вузла комутації з точки зору захисту інформації складається з двох підсистем:

– підсистема управління станцією;

– підсистема комутації абонентних і з'єднувальних ліній зв'язку.

Підсистема управління станцією містить у собі:

– спеціалізовані пристрої управління (CU/AM), які реалізують принцип програмного управління, і складаються з процесорів, внутрішньої та зовнішньої пам'яті, периферійних пристроїв, спеціалізованих модулів управління сигналізацією, оброблення викликів, надання послуг і деяких інших програмно-апаратних компонентів, які є характерними для комп'ютерної техніки;

– термінали обслуговування (tty) приєднані до пристроїв управління через канали технологічного обслуговування (com port) та до підсистеми комутації через канали інформаційного обслуговування абонентів (channel).

Підсистема комутації містить у собі пристрої, які реалізують процеси комутації (TM-switch), мультиплексування та концентрації абонентських і з'єднувальних ліній (TSI), а також компоненти обладнання абонентських ліній зв'язку – абонентські прикінцеві пристрої (terminal), фізичні лінії зв'язку (trunks), пристрої абонентських ліній (AIU), станційні абонентські комплекти (LP) і тому подібне.

На виходах підсистеми управління утворюються в реальному часі потоки технологічних сигналів (команди та звіти), за допомогою яких здійснюється управління підсистемою комутації. З іншого боку, абонентські прикінцеві пристрої обмінюються управляючою інформацією з підсистемою управління станцією через канали управління з'єднанням (signaling).

Потенційні види загроз інформаційним ресурсам у вузлі комутації мають свої особливості, крім загальновідомих порушень конфіденційності, цілісності, порушення доступності (відмова в обслуговуванні), спостережності (керованості) станції, необхідні заходи захисту від несанкціонованого користування інформаційними ресурсами станції (зокрема, несанкціоноване користування послугами, які надаються тощо).

Реалізація загроз для інформаційних ресурсів вузла комутації на базі системи 5ESS може здійснюватися:

– шляхом НСД до інформаційних ресурсів вузла комутації, коли порушуються встановлені правила розмежування доступу з метою реалізації будь-яких з видів загроз через канал спеціального (неприпустимого регламентом) впливу за допомогою штатних засобів доступу;

– через канал спеціального (неприпустимого регламентом) впливу із застосуванням штатних основних програмних і технічних засобів станції (але не штатних засобів доступу) на обладнання, програми, дані і процеси з метою реалізації будь-яких з видів загроз для інформації вузла;

– через канал спеціального (неприпустимого регламентом) впливу на параметри середовища функціонування вузла з метою порушень доступності до інформації на вузлі комутації;

– через канал спеціального впливу на компоненти 5ESS за допомогою апаратних або програмних закладень, запроваджених в процесі її експлуатації з метою реалізації будь-яких із видів загроз;

– через канал спеціального впливу позаштатними програмними або технічними засобами на елементи обладнання, програми, дані і процеси вузла комутації, встановленими в процесі її експлуатації з метою реалізації будь-яких із видів загроз інформації вузла;

– через кількісну або якісну недостатність компонентів вузла комутації з метою реалізації будь-яких із видів загроз для інформації;

– за рахунок використання випадкових збоїв і відмов у роботі обладнання вузла комутації з метою реалізації будь-яких із видів загроз для інформаційних ресурсів;

– за рахунок використовування помилок і некоректних (зокрема, зловмисних) дій відповідальних осіб при зберіганні критичної інформації на фізичних носіях з метою реалізації будь-яких із видів загроз для інформаційних ресурсів на ЦКС.

Потенційні загрози інформаційним ресурсам вузла комутації, що специфічні для комутаційної системи 5ESS:

– НСД до операційної системи (програмного забезпечення підсистеми управління);

– НСД до системного термінала (tty), якій приєднано або може бути приєднано до підсистеми управління;

– НСД до модемної лінії доступу до модуля технічної експлуатації;

– перевантаження через лавиноподібне зростання числа телефонних викликів;

– НСД до фізичних носіїв інформації (жорсткі диски, магнітні стрічки) з програмним забезпеченням;

– НСД до станційного кроса;

– активізація нештатних додаткових видів обслуговування.

Об’єктами захисту інформаційних ресурсів вузла комутації на базі системи комутації 5ESS є:

– апаратні засоби, спеціальні впливи, на які через технічні канали і шляхом НСД, можуть привести до створення та реалізації загроз для інформаційних ресурсів:

– програмно-інформаційні компоненти, на яких знаходиться технологічна інформація, що підлягає захисту.

Елементи (модулі і блоки) вузла комутації 5ESS, які можуть бути об’єктами реалізації загроз, – це:

1. Адміністративний модуль (АМ).
2. Комутаційний модуль (СМ).
3. Комутаційні модулі (SM).
4. Станційний крос (DDF).
5. Обладнання електроживлення.

До специфічної інформації, яка підлягає захисту у вузлі комутації, відноситься:

1. Інформація про абонентів, яка обробляється і зберігається на станції.;
2. Технологічна інформація в підсистемі управління, зокрема інформація підсистеми захисту інформації.
3. Технологічна інформація в каналах сигналізації (signaling link).

Інформація про абонентів, яка є інформацією приватних осіб, та інформація, яка є власністю держави, у визначенні Закону України «Про інформацію» може належати до статистичної, правової, соціологічної інформації або інформації, що використовується для забезпечення діяльності державних органів (органів місцевого самоврядування). Згідно з постановою Кабінету Міністрів від 29.03.2006 № 373 під час оброблення у вузлі комутації така інформація повинна зберігати цілісність та доступність. Ця вимога досягається шляхом створення КСЗІ, яка забезпечує захист від несанкціонованих дій, які можуть привести до її випадкової або навмисної модифікації або знищення.

Технологічна інформація є власністю підприємства – власника вузла комутації і є конфіденційною. До неї висуваються вимоги конфіденційності, цілісності, доступності та спостережності.

Докладніший список конфіденційної інформації вузла комутації мобільного оператора такий.

Характеристика інформаційного середовища.

На ЦКС 5ESS циркулює інформація, яка підлягає захисту. До неї відносяться:

1) абонентна інформація;

2) технологічна інформація в підсистемі управління вузлом;

3) дані про базові станції мобільного зв’язку;

4) дані про канали (з’єднувальні лінії) з іншими вузлами комутації;

5) дані про абонентські послуги;

6) дані щодо оплати послуг зв’язку;

7) дані про абонентний трафік;

8) файли з програмним забезпеченням станції 5ESS (завантажувальні магнітні стрічки);

9) дані про конфігурацію обладнання вузла комутації;

10) дані підсистеми захисту інформації;

11) файли з протоколами роботи обслуговуючого персоналу (лог-файли команд інженерів);

12) файли з протоколами роботи технічних засобів вузла комутації;

13) технологічна інформація в каналах міжстанційної сигналізації.

Розмежування доступу різних категорій користувачів (інженерів вузла комутації) до типів ресурсів станції 5ESS встановлюється в межах задач кожного користувача, виходячи з таких правил:

– керівник або адміністратор безпеки вузла комутації має доступ до: інформаційних об’єктів, які містять загальнодоступну інформацію; службової інформації КСЗІ; засобів захисту інформаційних ресурсів, операційних систем і прикладного ПО; технічних засобів, які задіяні в технологічному процесі управління КСЗІ; інших об’єктів з правами доступу іншого адміністратора (для резервування цих функцій);

– технічний обслуговуючий персонал (користувач) вузла комутації має доступ до: інформаційних об’єктів, які містять загальнодоступну інформацію; інформаційних об’єктів, які містять технічну, проектну, експлуатаційну документацію; відповідних технічних засобів вузла для проведення робіт зо обслуговування й експлуатації.

Надання обслуговуючому персоналу (інженерам станції 5ESS) певного профілю атрибутів доступу, до певного ресурсу та його прав доступу здійснюється лише у випадках виконання таких умов:

– категорія користувача (інженера) відповідає рівню доступу до об’єкта захисту, як це визначено загальними правилами розмежування доступу;

– доступ до даного об’єкта захисту безумовно службовими обов’язками користувача (інженера);

– вид взаємодії користувача (інженера) з об’єктом захисту (перелік дій над об’єктом) встановлено як дозволений;

– вид взаємодії користувача (інженера) з об’єктом захисту визначено службовими обов’язками.

Заходи з забезпечення безпеки фізичного середовища вузла комутації мобільного оператора повинні відповідати вимогам категорії А (ДБН 78.11.001-98 «Укріплення об’єктів, які охороняються за допомогою пультів централізованого нагляду Державної служби охорони. Загальні технічні вимоги»).

Правила пожежної безпеки повинні відповідати вимогам НАПБ В.01.001-98/5.2.00 «Правила пожежної безпеки в галузі зв'язку».

Віддалене обладнання розміщено в шафах, які встановлюються в спеціально виділених фізично захищених приміщеннях.

Резервні носії інформації вузла комутації на магнітних стрічках або лазерних компакт-дисках повинні зберігатися в призначених для цього місцях у металевих шафах, приєднаних до системи заземлення. Не допускається зберігати такі носії на відкритих місцях, ящиках столів або в незакритих металевих шафах.

Питання для самоконтролю

1. Сформулюйте цілі та задачі інформаційної безпеки.
2. За якими принципами проектуються ситеми інформаційної безпеки сатанції 5ESS?
3. Опишіть архітектуру та основні технічні параметри системи комутації 5ESS з позиції інформаційної безпеки.
4. Поясніть порядок та результати обстеження вузла комутації.
5. Розкрийте можливі варіанти оброблення ризиків від реалізації загроз інформаціним ресурсам вузла комутації.
6. Опишіть модель загроз інформаціним ресурсам сатанції 5ESS.
7. Опишіть модель порушника інформаційної безпеки сатанції 5ESS.
8. Розкрийте рівень ризику від порушників різних категорій.
9. Розкрийте сутність методу очікуваних втрат.
10. Розкрийте порядок та результати вибору заходів захисту інформації на вузлі комутації.
11. Поясніть порядок планування заходів захисту інформації на вузлі.

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 вузла 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 викликів.

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 розробленні комплексу засобів комп’ютерно-телефонної інтеграції як сукупності рекомендацій та стандартів, спрямованих на взаємодію пристроїв телефонного зв’язку та комп’ютерної техніки. Крім 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, які користуються міжміським та міжнародним зв'язком, для вивільнення оператора від трудомістких монотонних операцій.

Залежно від характеру операції, які 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 дзвінку 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 розвиненої 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 між 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 факторів: збільшення швидкості оброблення викликів; раціональне використання високооплачуваних спеціалістів; скорочення чисельності операцій, що виконуються при обробленні 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 оброблення 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.

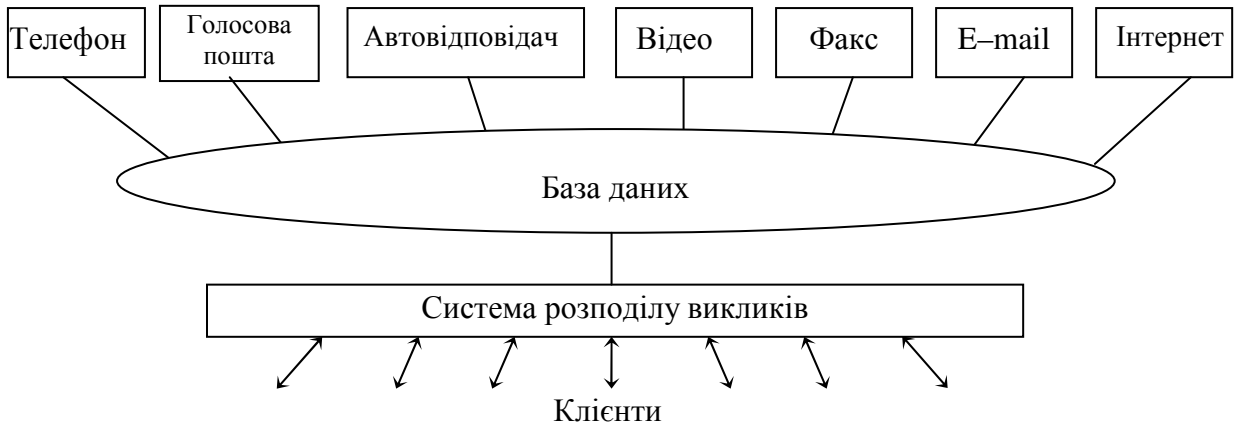

Рисунок 6.1 – Функціональна структура центру оброблення

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 оброблення.

Структура та принципи функціонування центрів оброблення викликів. Варіант архітектури ЦОВ подано на рис. 6.2.

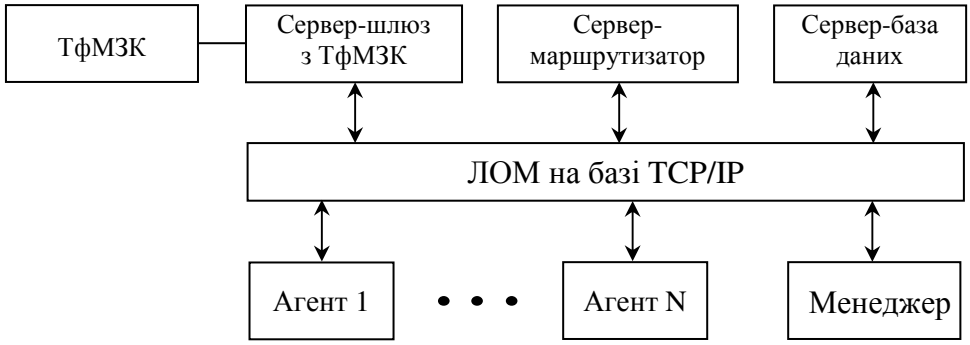

Рисунок 6.2 – Функціональна структура центру оброблення викликів

Перші варіанти побудови телефонно-комп'ютерного ЦОВ реалізовувались із застосуванням установчо-виробничої комутаційної станції та телекомунікаційного сервера.

Більш гнучкі ЦОВ можуть базуватись на застосуванні стандартів *Voise over IP* (наприклад Н.323, який регламентує протоколи передавання телефонії *IP*-мережею).

Продуктивність центру залежить від пропускної здатності його складових частин: шлюзу для з'єднання 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 ніж 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 з'єднання з комп'ютерною мережею. Його функція – забезпечити обмін повідомленнями між 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 дозвону, система інтерактивного голосового обміну, сервер баз даних та сервер статистики.

Комунікаційний сервер забезпечує можливість оброблення викликів і є безпосередньо з'єднанний 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 у 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, яка 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, які пишуться за допомогою спеціальних засобів з урахуванням змісту перших двох баз; API визначають призначення та експлуатаційні можливості ЦОВ і мають постійно оновлюватись.

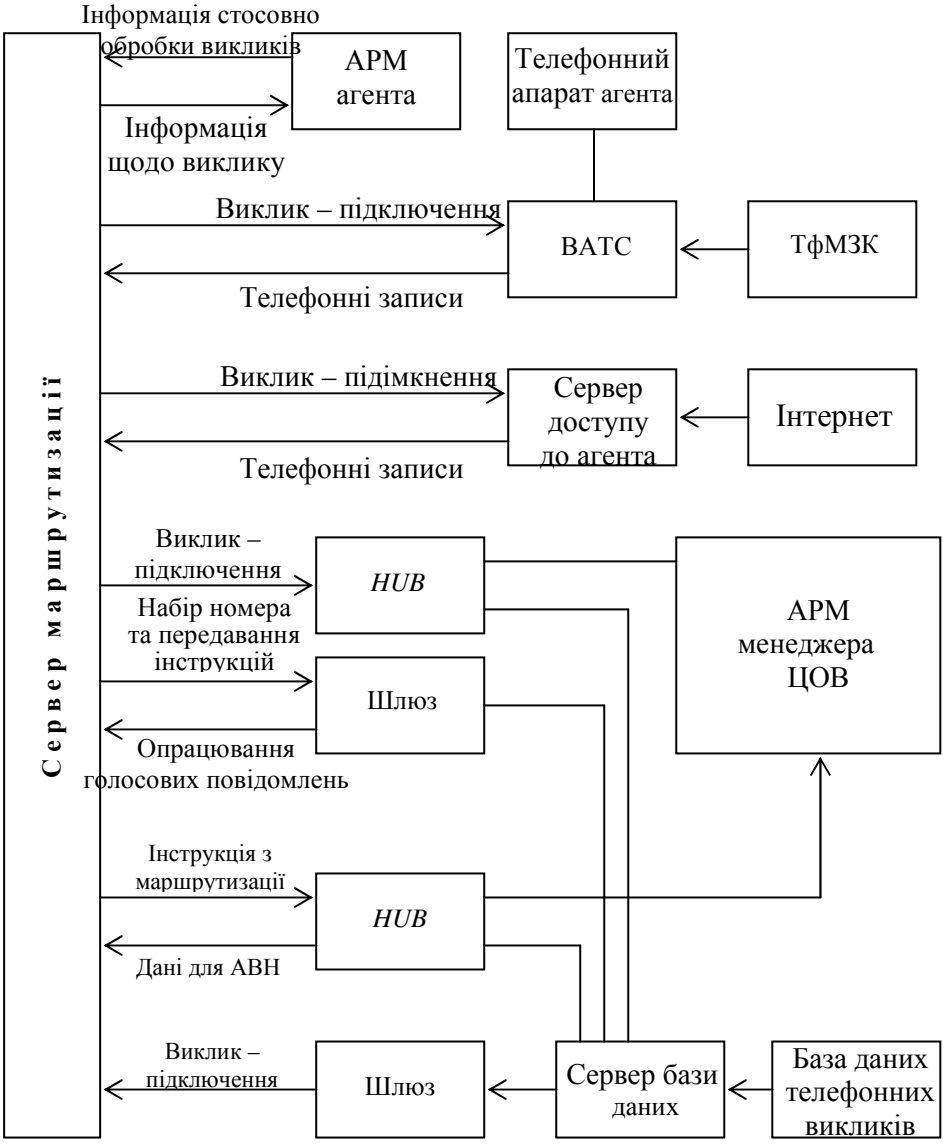

Рисунок 6.3 – Функціональна взаємодія апаратного та програмного забезпечення ЦОВ

HUB – це комутатори, які забезпечують з'єднання серверів та автоматизованих робочих місць (АРМ) для передавання сигналів

виклику – підключення, набір 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, який забезпечує систему голосового меню. Вибір пунктів меню споживач здійснює за допомогою клавіатури звичайного телефону в режимі тонального набору. Пристрій виконується у вигляді окремого блока і з'єднується 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 оброблення викликів служби «Міліція» на базі відомчої ЦАТС

Операторський центр оброблення викликів служби «Міліція» може бути побудований як показано на рис. 6.4. Фізично виклики розподіляються за робочими місцями – консолями [24].

Консоль може бути реалізована різними способами, залежно від апаратно-програмних рішень, застосованих в обладнанні 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 зі спеціалізованою базою даних служби «Міліція». У 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 оброблення 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, позв'язану з викликом (номер викликаючого абонента, дані, отримані під час діалогу з IVR і т. д.), й 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, питання що цікавить, попередня історія і т. п.), прочитується з бази даних центру і з'являється на екрані робочого місця оператора (автоматично або за його командою). 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 установленого нею за списком сповіщення.

Оператор (контролер) служби «Міліція», має право не тільки займатися обслуговуванням викликів, що надходять від абонентів, але і

контролювати роботу операторів у групі (підключившись у режимі прихованого прослуховування й аналізуючи статистичну та оперативну інформацію).

Сповіщення про вхідний виклик може бути передано на робоче місце оператора двома способами:

– за допомогою візуальної індикації;

– тональним сигналом, що посланий 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 поділити на три основні категорії: оперативна, статистична, облік викликів.

Оперативна інформація дозволяє керівництву служби «102» контролювати функціонування обладнання, 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 й 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, обслугованих 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 у черзі); середня інтенсивність повторних викликів; ідентифікаційний номер оператора, що обслужив виклик; номер групи операторів; відсоток обслугованих викликів.

Суттєвою 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 з загальними міліційними інформаційними базами даних. Для обслуговування кожного виклику, будь він що вхідний чи 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), позв'язаних між собою високошвидкісними каналами передачі даних (щоб забезпечувалася робота із загальними базами даних).

Існує ціла низка способів реалізації такого універсального доступу. Одним з найперспективніших й 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*-сайта з Інтернет. При цьому користувач й оператор *Call*-центру можуть вести діалог і навіть синхронно проглядати одні і ті ж *Web*-сторінки (рис. 6.4).

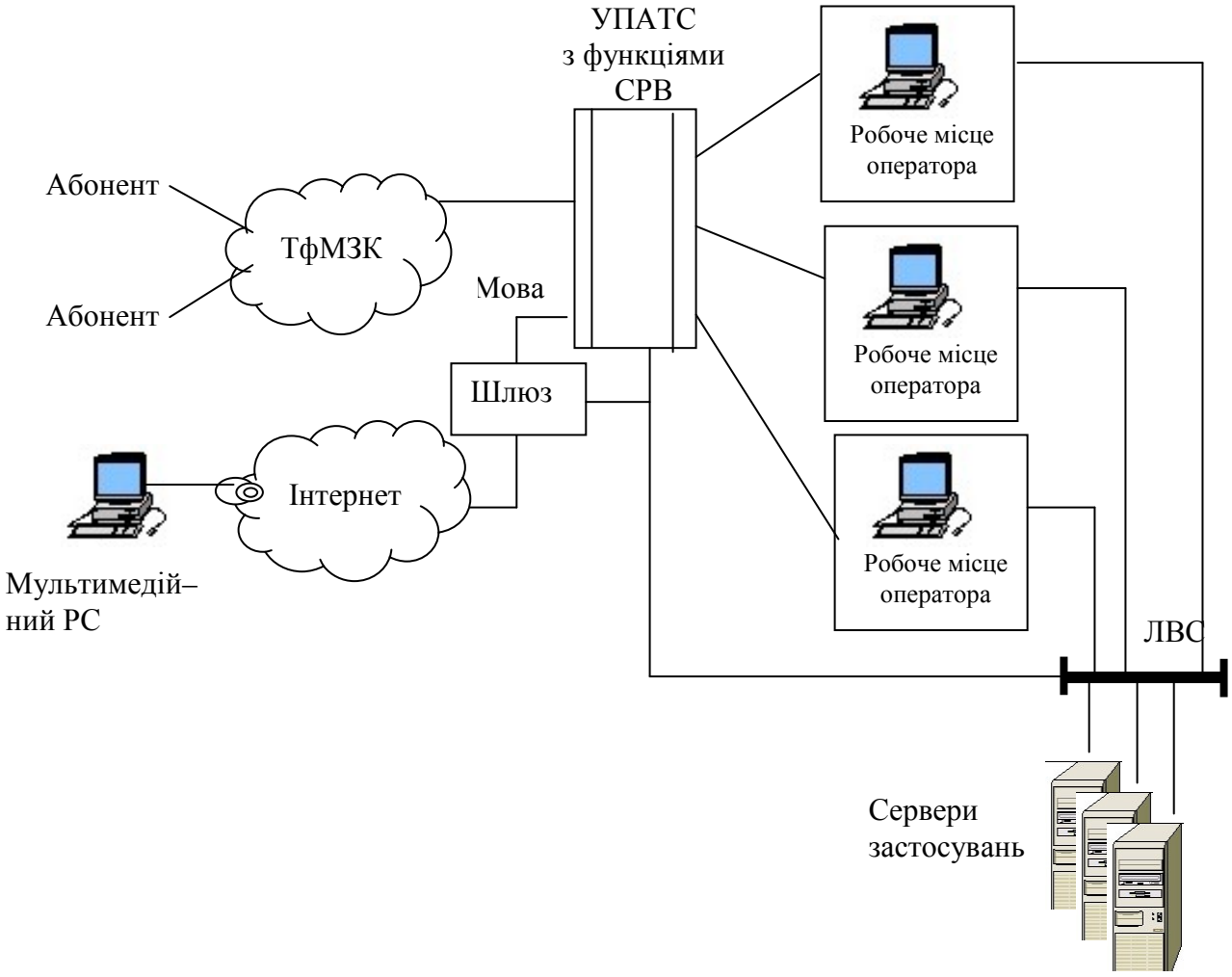

Рисунок 6.4 – Варіанти доступу до контакт-центру служби «Міліція»

Під час виклику із Інтернет користувач отримує доступ до *Call*-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.

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 суттєво збільшити продуктивність *Call* - центру, причому зробити це не за рахунок збільшення числа операторів, а за рахунок оброблення 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 сервера, 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, визначених управляючим застосуванням.

Коли звільняється оператор, здатний обслужити виклик цього типу і тематики, «виклик» електронної пошти надходить до термінала оператора, і той отримує повідомлення про його присутність на екрані браузера. Призначений для користувача інтерфейс робочого місця оператора *Call*-центру містить низку інструментальних засобів, за допомогою яких оператор має нагоду створити відповідь для передачі його по електронній пошті, перевести «виклик» в режим утримання для наведення довідки у інших операторів *Call*-центру або переправити «виклик» іншому оператору, що вважається фахівцем у даній області. Під час виконання всіх цих дій оператор, зайнятий обслуговуванням виклику, що надійшов у вигляді електронного листа, вважається зайнятим, й інші виклики надходити 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 надходять з різних телекомунікаційних мереж:

– мовного зв’язку – з ТфМЗК;

– мовного зв’язку – з Інтернет, з використанням технології *IP*-телефонії;

– зв’язку факсом, електронною поштою;

– відеовикликів (в недалекій перспективі).

Мультимедійність починається з доступу до послуг контакт-центрів.

Розглянемо деякі зі 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*-сайта 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 чата, 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 й 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 спектра можливостей як в плані доступу, так і з погляду послуг, що надаються, з використанням людських ресурсів (операторів) й 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 обладнання 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) та взаємодіючими в процесі обслуговування виклику з інформаційними і технологічними базами даних. При цьому кожний з таких серверів відповідає за свій набір послуг (СРВ, *IVR* і ін.). Так само розв'язуються питання надійності (стандартні методи резервування апаратного забезпечення комп'ютерної техніки); масштабування (установка, за необхідності, серверів застосувань, що працюють в режимі розподілу навантаження); введення нових функцій (додаткові сервери і застосування); створення розподілених систем (достатньо позв'язати різні офіси однією комп'ютерною мережею, що володіє потрібною пропускною здатністю).

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, приймання й оброблення викликів, що надходять 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 ефективним оброблення викликів з різних середовищ і забезпечує необхідну якість обслуговування. Якщо взяти до уваги й інші переваги *IP*-контакт-центрів, у тому числі низьку вартість розгортання та ефективність масштабування, привабливість використовування в контакт-центрах пакетної комутації стає очевидною.

У той самий час віртуальна природа *IP*-адресації в сучасних контакт-центрах дозволяє легко вирішувати 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.

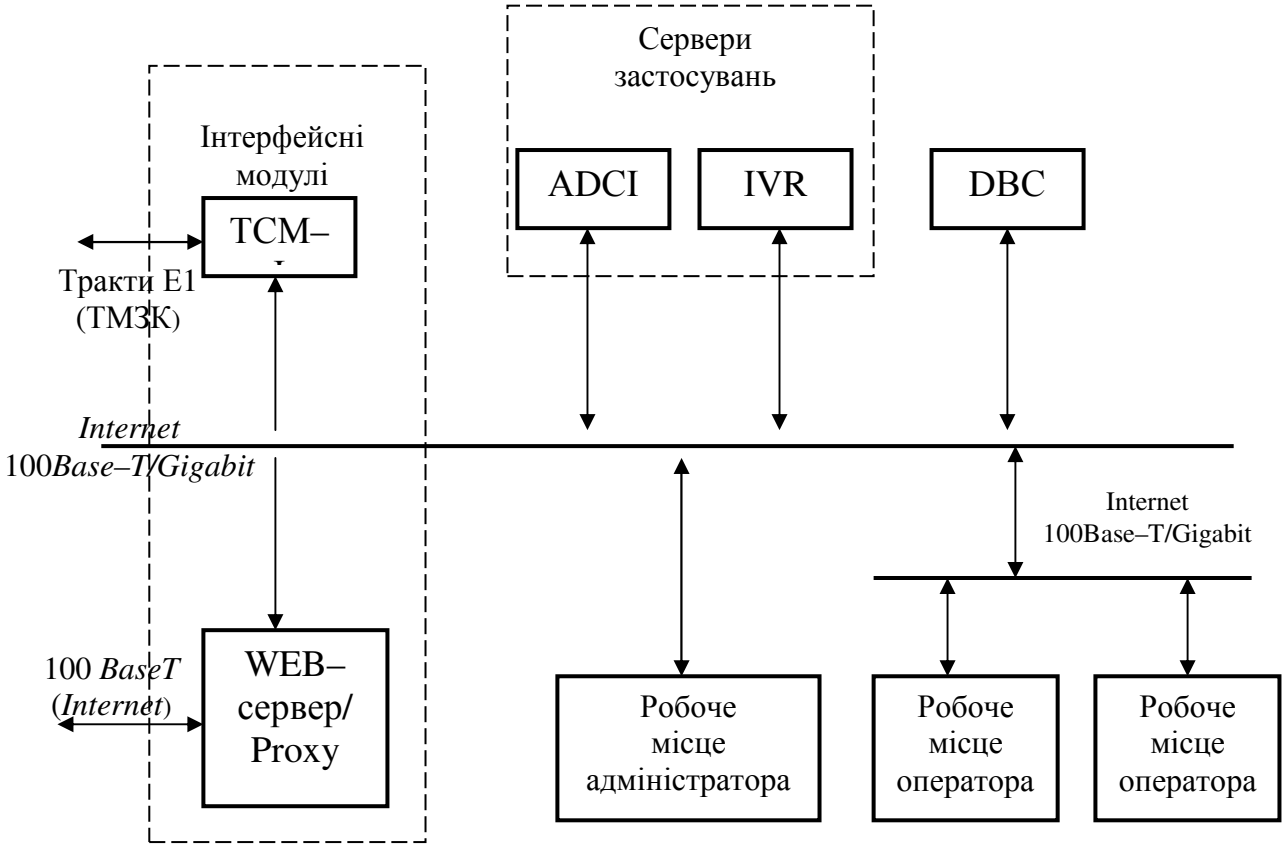

Рисунок 6.5 – Типова структура *IP*-контакт-центру служби «102» Міліція

Очевидні переваги контакт-центру з погляду витрат на організацію вилучених 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 надходить з боку ТфМЗК, у вигляд, придатний для передавання по мережах з маршрутизацією пакетів *IP*: кодування й упакування 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 обладнанням ТфМЗК, так і з пристроями, що працюють за стандартами *IP*-телефонії H.323 чи *SIP*.

Як правило, при використовуванні *IVR* алгоритми оброблення викликів в операторському центрі передбачають передачу абонентам, які чекають в черзі, аудіоінформації, наприклад, мовних фраз. Ці фрази можуть містити відомості про порядковий номер виклику в черзі й орієнтовному часі очікування. Крім того, цілком можливо, що, прослуховуючи такі фрази, абонент отримає 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 повністю функціональною і задовольняла вимогам, про які йшла мова 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 функцій, 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 й 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) зі спеціалізованим програмним забезпеченням. За його допомогою виконуються функції конфігурації і діагностики системи, контроль стану інтерфейсів і розмовних каналів, збирання оперативної і

статистичної інформації про роботу системи й обслуговування викликів, а також генерація звітів і архівація.

6.3.5 Робочі місця операторів

Консолі операторів організовуються на базі стандартних персональних комп'ютерів з установленим 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 надходить 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 у групі, що мають нагоду кваліфіковано обробити запит, виклик ставиться 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 приблизний час 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 у 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 у 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 Інтернет як засобу доступу до інформації обумовлює необхідність наявності в архітектурі будь-якого сучасного операторського центру *Web*-сервера, через який користувачі операторського центру можуть отримувати доступ до послуг через мережу Інтернет.

Абонент, який охоче отримае необхідну інформацію, використовуючи ресурси контакт-центру про будь-які 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 оброблення виклику в комп'ютер користувача для запуску застосування *IP*-телефонії. *Java*-застосування забезпечує інтерфейс, через який користувач може також отримувати 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 надходить з телефонної мережі.

6.4.2 Алгоритм обслуговування виклику в режимі «Call-back»

Режим відкладеного обслуговування передбачає можливість поставити виклик в чергу на обслуговування без необхідності його утримання з подальшим зворотним викликом вільного оператора до абонента. Абонент може замовити зворотний виклик з інформаційного сайта служби «Міліція», наприклад, паспортного столу.

При замовленні зворотного виклику з *Web*-сайта 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 ефективне оброблення всіх видів трафіка, 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 трафіка (наприклад, для реалізації алгоритму обслуговування абонентів за системою зі 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 за сформованими активними списками сповіщення, визначає стан номера викликуваного 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 за оператором

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 у системі, підтримують можливість розподілу операторів за кваліфікацією, що дозволяє ефективно здійснювати оброблення заявок. Крім того, система може бути гнучко набудована під конкретні вимоги замовника.

6.4.6 Можливості операторів у системі

У системі передбачена організація декількох груп операторів служби «Міліція». В групі може бути одне або декілька робочих місць операторів. Оператори у системі ідентифікуються унікальним номером (ім'ям) і мають свій пароль. Підтримується розподіл на операторів і старших операторів, які володіють різними правами доступу.

Оператору центру надаються наступні можливості:

– реєстрація в необхідній групі на будь-якому робочому місці за 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 викликуваного абонента. Забезпечується можливість регістрації заявки, що надійшла, шляхом заповнення «ситуативної карти» з використанням технології взпливаючого вікна.

Відомості про того, хто дзвонить:

– номер викликуваного абонента;

– адреса, за яким зареєстрований телефон;

– у випадку, якщо телефон домашній:

– ПІП (і можливо паспортні дані) абонента, на якого зареєстрований номер;

– список осіб, зареєстрованих за даною адресою, наявність у них зброї, судимості, транспорту.

Відомості про подію:

– адреса, де вчинено правопорушення;

– ПІП всіх громадян, приписаних за цією адресою;

– наявність судимості і зброї; транспорт.

6.4.7 Можливості старшого оператора

1. Старший оператор служби «Міліція» має нагоду контролювати процес прийому й обслуговування викликів, для чого йому надається наступна інформація:

– стан операторів у своїй службі/групі;

– стан черги;

– статистика щодо вибраного оператора (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 розмов операторів з абонентами з можливістю подальшого прослуховування з комп'ютера старшого оператора. Функція запису розмови доступна також звичайному 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 за різними критеріями: 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 отримувати 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 у 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 у системі передбачені гнучкі алгоритми маршрутизації. Настройка того або іншого алгоритму здійснюється на основі аналізу цілей і параметрів запровадження МЦОВ.

6.4.10 Збірання статистичної інформації й облік викликів

У системі передбачено формування, зберігання чисельної статистичної і експлуатаційної інформації, а також можливість генерації звітів реального часу і хронологічних довгострокових звітів.

Інформацію у системі можна поділити 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 з замовником). Можлива генерація звітів реального часу і хронологічних довгострокових звітів. Звіти формуються по запитах з робочого місця адміністратора системи. Генерація звітів може проводитися за годинами, добою, тижнями і т.д.

Можливе збірання різноманітної статистичної інформації за тим, хто дзвонить, 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 (обслугований/втрачений);

– етап обслуговування, на якому виклик був втрачений (для втрачених_викликів);

– ініціатор відбою;

– за необхідності створюється ситуаційна карта.

У режимі реального часу передбачена видача наступних типів звітів:

– стан всіх операторів у групі;

– стан всіх робочих місць МЦОВ;

– стан черг до кожної групи операторів.

Крім того, в реальному масштабі часу старший оператор має нагоду отримати інформацію за часом очікування викликів у черзі, середньої тривалістю розмови і т.д.

Система генерує наступні типи хронологічних звітів:

– інформація за кількістю будь-якого типу викликів, що пройшли через систему (вхідний/внутрішній/вихідний) за будь-який проміжок часу;

– інформація за статусом викликів: скільки за певний проміжок часу викликів було обслуговано/втрачено/необслуговано;

– 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 усіма операторами групи/служби сумарно за будь-який проміжок часу;

– сумарна зайнятість одного/всіх операторів за робочу зміну (за часом);

– кількість переадресацій внаслідок зайнятості всіх операторів за будь-який проміжок часу;

– розподіл часу оператора на обробку різних типів викликів.

Забезпечуються генерація звітів зао годинами, добою, тижнями, місяцями, кварталами, зберігання в базі даних МЦОВ архівної інформації про установлені з'єднання, а також статистичної інформації за період 8 місяців, обсяг БД може бути збільшений за узгодженням з 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-центру, 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 тощо, для чого в контакт-центрі є спеціалізована підсистема звітності й адміністративного управління.

Разом з операторами і старшими операторами у 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 й атрибутами груп операторів (визначення складу операторів, що входять до групи; завдання пріоритету групи і тощо);

– 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 та іншими голосовими підказками;

– настройка параметрів інтерфейсу з опорною АТС;

– настройка «чорних списків» абонентів, яким заборонено обслуговування у системі.

6.5 Розрахунок якості обслуговування та кількості операторів

Характеристики доставки інформації та послуг користувачам в узагальненому вигляді входять до показників доступності і, частково, до показників 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. Припустимо, 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 Краруп 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, ніж довгі. Найпростіший потік задає важчий режим роботи, ніж 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 із фізичних тлумачень є те, що інтенсивність навантаження, виражена в Ерлангах, характеризує середню ефективність використання системи. При цьому 1 Ерл – це одне годинно-зайняття 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 з найпростішим потоком 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, роботу автоматизованих систем відповіді і власне агентів. На підставі сценаріїв потрібно визначити середню тривалість кожного виклику та середній час зайнятості агента при обробленні 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, наприклад, 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 з’єднання 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 залишає систему, якщо всі обслуговуючі пристрої зайнято. Ймовірність блокування запиту задається відомою формулою Ерланга першого роду, що добре табульована [27]:

$$p(n) = \frac{\frac{a^n}{n!}}{\sum_{\nu=0}^{n} \frac{a^\nu}{\nu!}}. \tag{6.6}$$

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 виду:

$$P(>0) = \left(\frac{a^n}{n!} \frac{n}{n-a} \right) : \left[\sum_{\nu=0}^{n-1} \frac{a^\nu}{\nu!} + \frac{a^n}{n!} \frac{n}{n-a} \right]. \tag{6.7}$$

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

$$T = \frac{P(>0)}{\mu(n-a)}. \tag{6.9}$$

Проведемо обчислення кількості агентів, необхідних для обслуговування запитів за різних систем обслуговування. Нехай у системі з блокуванням необхідно забезпечити якість обслуговування таку, щоб 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

$$P(>0) = T\mu(n-a) = 1/3(n-9). \tag{6.10}$$

Маємо в результаті 12 операторів.

Отже, системи з очікуванням забезпечують більш високе використання обладнання.

На відміну від традиційних телефонних систем, які 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

$$h(t) = \frac{(f\mu t)^{f-1}}{(f-1)!} e^{-f\mu t} f\mu . \qquad (6.11)$$

При $f = 1$ маємо показовий закон розподілу, а випадок $f = \infty$ відповідає постійному часоу обслуговування.

Детальні математичні рішення знайдено для систем масового обслуговування з очікуванням, які 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 значною кількістю з інтенсивністю λ в 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

$$L = a + (a^2 + \lambda^2\sigma^2)/2(1 - a), \qquad (6.12)$$

де $a = \lambda\mu$.

Середня довжина черги обчислюється як

$$L_ч = a + (a^2 + \lambda^2\sigma^2)/2(1 - a), \qquad (6.13)$$

а середній час очікування як

$$W = (a^2 + \lambda^2\sigma^2)/2\lambda(1 - a). \qquad (6.14)$$

Якщо час обслуговування має показовий розподіл, то

$$L = a/(1 - a);\ W = a/\mu\ (1 - a). \qquad (6.15)$$

А якщо час обслуговування постійний, то

$$L = (2 - a)/2(1 - a);\ W = a/2\mu\ (1 - a). \qquad (6.16)$$

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 управління 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 оброблення викликів і контакт-центру повинна бути частиною політики інформаційної безпеки органу внутрішніх справ і бути взаємоузгодженими. Розглянемо загрози і вимоги до системи інформаційної безпеки органу внутрішніх справ.

Загрози інформаційної безпеки. Виникаючі в процесі діяльності органу внутрішніх справ загрози поділяються за характером джерела на два базові класи – зовнішні і внутрішні. До першого відносяться наступні види загроз:

1а) загрози фізичного проникнення сторонніх осіб з метою розкрадання критичної інформації на різних носіях;

1б) загрози проникнення в корпоративну мережу з метою отримання разового або постійного доступу до критичної інформації;

1в) загрози різних зовнішніх дій на корпоративну мережу з метою дезорганізації її роботи, нанесення матеріального збитку різноманітними способами;

1г) загрози впровадження в корпоративну мережу ззовні з метою використання її ресурсів в особистих цілях;

1д) загрози зняття інформації з працюючих комп'ютерів шляхом візуального спостереження і сканування їх електромагнітних або сонарних сигнатур.

До другого класу відносяться наступні види загроз:

2а) загроза нелояльної поведінки персоналу за корисливими або особистими мотивами, що приводить до просочування критичної інформації або порушень режиму забезпечення загальної безпеки;

2б) загрози порушення захисту від несанкціонованого доступу до корпоративної мережі внаслідок халатності або низького професійного рівня персоналу;

2в) загрози проведення ними прямих диверсійних дій або саботажу з боку персоналу, схиленого до співпраці сторонними особами або організаціями;

2г) загрози появи (застосування) в процесі звільнення (особливо внаслідок 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;

2д) загрози використання персоналом ресурсів корпоративної мережі й оброблюваної в ній інформації в особистих цілях;

2е) 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 описаних видів загроз можливі наступні методи протидії їм:

– 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 й 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, якими корпоративна мережа може з'єднуватися 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 суворо тільки необхідні ресурси;

– виділити експлуатований *WWW*-сервер в окремий ізольований сегмент, а за 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 розніми, 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 суворо 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 обробленні критичної інформації;

– для збереження найкритичнішої інформації яка зберігається на носіях, так і переміщається по мережі, застосовувати криптографічне програмне забезпечення, що використовує сучасні алгоритми шифрування;

– постійно сканувати простір корпоративної мережі і поступаючу 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 відома колективу, акцентувати увагу персоналу на тому, що розповсюдження шкідливих програм (вірусів) і порушення правил експлуатації комп'ютерів та їхніх 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 у 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 сервери, 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 у 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 вжити заходи по негайному реагуванню;

– систематично перевіряти дотримання режиму інформаційної безпеки – збереження печаток на обладнанні, 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), *We*b-сервер і доступ до Інтернет.

Потрібно: розмежувати права доступу на рівні відділів/підрозділів до ресурсів інших підрозділів і забезпечити безпеку при роботі з Інтернетом в плані несанкціонованого доступу з Інтернету до внутрішньої мережі організації.

Пропонується наступне рішення: мережа організації розбивається на сегменти за допомогою збиранню сегментів мережі на РІЗНИХ концентраторах (хабах). Усередині одного сегмента передбачається, що всі машини мають однаковий рівень доступу. В центрі мережі ставиться машина під ОС Linux з набудованими правилами фільтрації. Для кожного сегмента у сервері передбачається окрема мережна платня.

Доступ з одного сегмента в інший може бути дозволений або заборонений повністю або частково. Під частковим обмеженням доступу слід розуміти наступні види обмежень:

1. За *IP*-адресою джерела і приймача пакета.
2. За протоколом *TCP*/*UDP*/*ICMP*.
3. Зао портом джерела і приймача пакета.
4. За ознакою *SYN*/*ACK* (ініціатор/відповідач).
5. За інтерфейсами 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 ускладнює просту перестановку *IP*-адреси навіть

усередині одного сегмента 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 наведений на рис. 6.6.

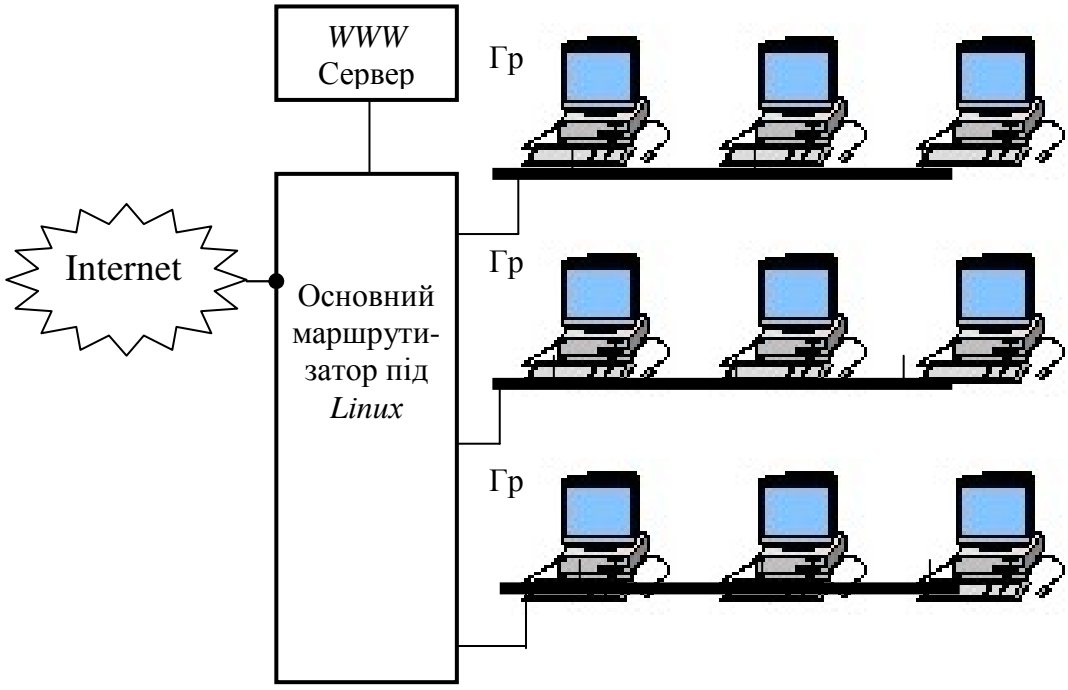

Рисунок 6.6 – Приклад сегментації мережі

На рис. 6.6 показано три підмережі для організації трьох поділених сегментів, внутрішній трафік яких не може прослуховуватися в режимі сніффування з іншого сегмента мережі. *WWW*-сервер в цьому 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*-сервера 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 робочої станції. Доступ для адміністрування може бути додатково захищено від прослуховування трафіка усередині свого сегмента.

Всі вищеперелічені 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 в Інтернет, 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 в міру необхідності.

Умовний кошторис проведення робіт щодо забезпечення режиму інформаційної безпеки. Кошторис складемо в умовних витратних одиницях (УВО).

Технічні засоби і заходи:

– придбання контейнерів типу *Mobil rack* , 2–3 шт. по 10–15 УВО;

– виготовлення нестандартних рознімів зовнішніх інтерфейсів (*LPT*) і ключів до них, 7-9 УВО за комплект;

– придбання комп'ютера-маршрутизатора і мережних апаратних засобів до нього, 700-1000 УВО;

– придбання зовнішнього накопичувача з інтерфейсом *LPT*, 140-175 УВО;

– відключення накопичувачів на змінних носіях, зовнішніх інтерфейсних роз'єднувачів, за потребою;

– виготовлення й установлення обладнання для опечатання корпусів комп'ютерів, контейнерів з вінчестерами, виготовлення (закупівля) пеналів для зберігання ключів рознімів LPT, за потребою;

– установлення на вікнах у приміщеннях з комп'ютерами захисних жалюзі, за потребою;

– органолептичний контроль наявності сторонніх закладок на робочих станціях мережі, 2-4 УВО на робоче місце.

Програмні засоби:

– установлення і конфігурація програмного забезпечення маршрутизатора і брандмауера, 200 УВО;

– розробка, установлення, конфігурація засобів об'єктивного контролю робочих місць мережі, 4 УВО на робоче місце;

– установлення і конфігурація POP/SMTP і HTTP серверів і засобів об'єктивного контролю на них, 100 УВО;

– конфігурація системи розмежування доступу користувачів, 50 УВО;

– установлення і конфігурація системи типу *packet sniffer* для роботи в режимі сканування мережі, 150 УВО;

– установлення системи моніторингу руху пакетів у корпоративній мережі і доступу до критичної інформації, 60 УВО;

– придбання антивірусу AVP з річною підпискою, 100 УВО;

– придбання антивірусу DoctorWEB, за потребою;

– установлення і конфігурація засобів шифрування даних, за потребою.

Далі перейдемо до розгляду процедур проектування системи інформаційної безпеки центрів оброблення викликів та контакт-центрів.

6.7 Комплексна система інформаційної безпеки центрів оброблення викликів

Модель безпеки центрів оброблення 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 ускладнюють 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 значний 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 оброблення 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 з 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 забезпечувати реєстрацію у системному журналі визначених політикою відповідних послуг 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 за аналогією 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, наприклад 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, наприклад для отримання інформації споживача;

– відмова оператора зв'язку від того, що функціональний об'єкт передав чи отримав дані щодо оплати або іншу інформацію;

– маскування, заи якого 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 в оплаті тощо.

Модель захисту інформаційних ресурсів ЦОВ розробляється на стадії технічного проектування. Вибір моделі захисту являє собою розв'язання задачі з мінімізації ресурсів захисту при забезпеченні

наведеного в технічному завданні рівня захищеності інформаційних ресурсів ЦОВ. У результаті розв'язання 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 зі 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 дотримання 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: НІ-2 – одиничне 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.

Розв'язання 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 передавання даних використовують технології створення резервних копій програм та даних і технології, що забезпечують гарантоване зберігання даних.

Питання для самоконтролю

1. Дайте визначення, що є центром оброблення викликів (ЦОВ) та його призначення.
2. Поясніть функції центру оброблення 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.
6. Як розрахувати показники якості обслуговування ЦОВ?
7. Як розрахувати кількість операторів ЦОВ?
8. Сформулюйте вимоги до ТЗІ в органах внутрішніх справ.
9. Опишіть структуру системи інформаційної безпеки ЦОВ.

7 ОСОБЛИВОСТІ ПРАКТИЧНИХ РЕАЛІЗАЦІЙ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЦАТС РІЗНИХ ТИПІВ

7.1 Система захисту інформації центру комутації рухомого зв'язку HUAWEI CDMA M800

7.1.1 Структура мережі

Центр комутації рухомого зв'язку CDMA M800 (далі M800 CDMA MSC) є ядром системи рухомого зв'язку CDMA, підтримує інтерфейси з іншими мережами і з різними функціональними елементами усередині системи CDMA. Центр комутації M800 CDMA MSC виконує функції управління рухливістю (ММ), функції комутації каналів зв'язку між рухомими абонентами даної системи або між рухомими абонентами системи й абонентами ТФОП. Положення MSC у структурі мережі показано на рис. 7.1

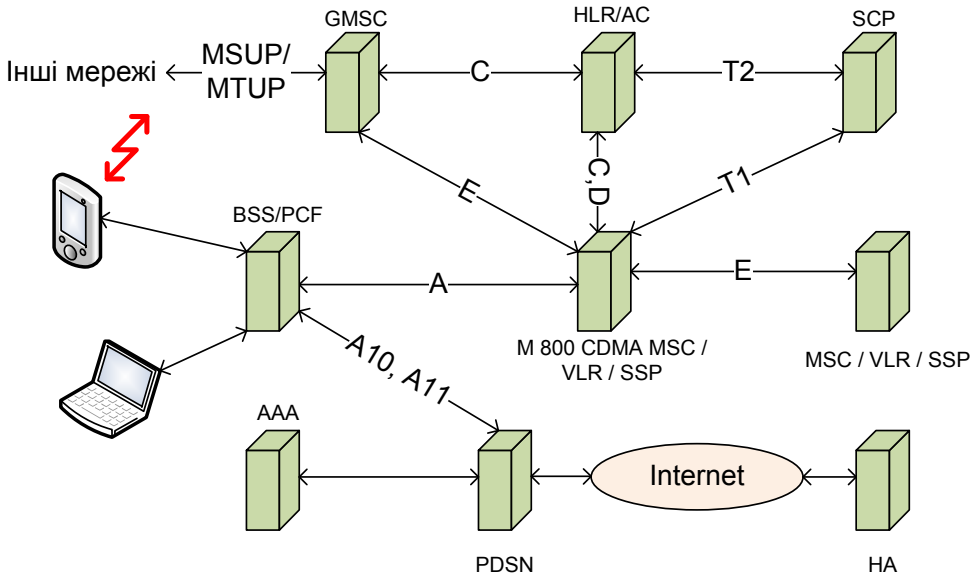

Рисунок 7.1 – Структура мережі

MSC: центр комутації рухомого зв'язку. Як ядро підсистеми комутації MSC виконує такі функції: встановлення викликів, вибір маршрутів, управління викликами, розподіл радіоресурсів, управління рухливістю, реєстрація місцезнаходження, управління хендоверами (естафетним передаванням управління). Крім того, MSC формує дані розрахунків з абонентами, управляє доступом абонентів до телефонної мережі загального користування (ТФЗК) та до послуг мережі, підтримує інтерфейс з іншими мережами за протоколом ОКС № 7.

VLR: Регістр тимчасового місцезнаходження. Як динамічна база даних VLR забезпечує зберігання тимчасової інформації (дані, необхідні для установлення викликів) щодо користувачів, приписаних до інших мереж, і що знаходяться в даний момент в зоні обслуговування MSC.

Оскільки VLR призначений для зберігання даних, необхідних для функціонування MSC, конструктивно його об’єднано з MSC.

BSS/PCF (підсистема базових станций/ вузол управління пакетною передачею даних) забезпечує радіодоступ рухомих абонентів до послуг підсистеми комутації. До складу BSS входять базові станції BTS і контролер базових станцій BSC.

AAA: Центр авторизації, аутентифікації й аудиту. Вузол автентифікації, авторизації та аудиту AAA є віддаленим сервером, що виконує функції автентифікації користувачів, авторизації та тарифікації доступу користувачів до послуг передавання даних і до додаткових послуг. Сервер володіє високою продуктивністю, підтримує різні бази даних, гнучкі методи оброблення даних і виконує функції proxy-сервера.

GMSC: Шлюз MSC. Шлюз MSC (GMSC) виконує функції маршрутизації, запрошує необхідну інформацію щодо маршрутів, забезпечує взаємодію з іншими мережами.

HLR: Опорний регістр місцезнаходження. Опорний регістр місцезнаходження HLR виконує функції бази даних для зберігання інформації, що використовується в процедурах управління рухомими абонентами, зокрема в регістрі зберігається інформація щодо послуг, на які підписався абонент, інформація про статус абонента, інформація щодо місцезнаходження MS, інформація про ідентифікатори MDN, IMSI (MIN) тощо. Центр автентифікації AC є одним із вузлів HLR, конструктивно вони виконані у вигляді одного виробу. Центр автентифікації забезпечує безпеку інформації у системі CDMA. В AC зберігаються автентифікаційні параметри, ключі шифрування, що дозволяє захистити систему від несанкціонованого доступу до інформації та до радіоресурсів.

SCP: Вузол управління послугами. Вузол комутації послуг (SSP) приймає запит на послугу інтелектуальної мережі (IN), який потім транслюється на SCP. SCP активізує певний модуль підтримки послуг та інформує про це SSP. Після відповіді SSP SCP запускає певну процедуру оброблення виклику з наданням запрошеної послуги. У підсистемі комутації M800 CDMA MSC вузол комутації послуг SSP також конструктивно об’єднано з MSC/VLR.

PDSN: Вузол обслуговування пакетногої передаванняі даних. Вузол обслуговування пакетного передавання даних PDSN виконує функції шлюзу між мережею бездротового доступу і базовою мережею IP, дозволяє організувати доступ рухомих абонентів до послуг передачі пакетних даних у мережах Internet/Intranet.

HA: агент опорної мережі. Агент опорної мережі HA виконує функції інтерфейсу між системою 3G та мережею Internet, дозволяє організувати доступ рухомих IP-користувачів до мережі Internet. HA може працювати в двох режимах «хост –> MN» і «MN –> хост».

7.1.2 Функції інформаційної безпеки

Підтримуються наступні функції інформаційної безпеки:

– автентифікація мобільного комутатора (MS) при його реєстрації;
– аутентифікація MS при установленні вихідного виклику;
– періодичне оновлення бази даних комутації послуг (SSD);
– автентифікація MS при установленні вхідного виклику;
– автентифікація при запиті додаткової послуги;
– процедура обчислення унікальної відповіді на запит;
– використання спільних для базового комутатора BS та мобільного комутатора MS даних засекречування SSD.

7.1.3 Архітектура програмного забезпечення

Структура програмного забезпечення центру комутації рухомого зв'язку CDMA M800 показана на рис. 7.2. Структура програмного забезпечення є багаторівневою, ранги рівнів, зображених на рисунку, зростають від центру до краю кола. Рівні програмного забезпечення в порядку зростання їх рангу: апаратні засоби й інтегроване в них програмне забезпечення, операційна система (OS), модуль управління зв'язком (CCM), інші функціональні програмні модулі.

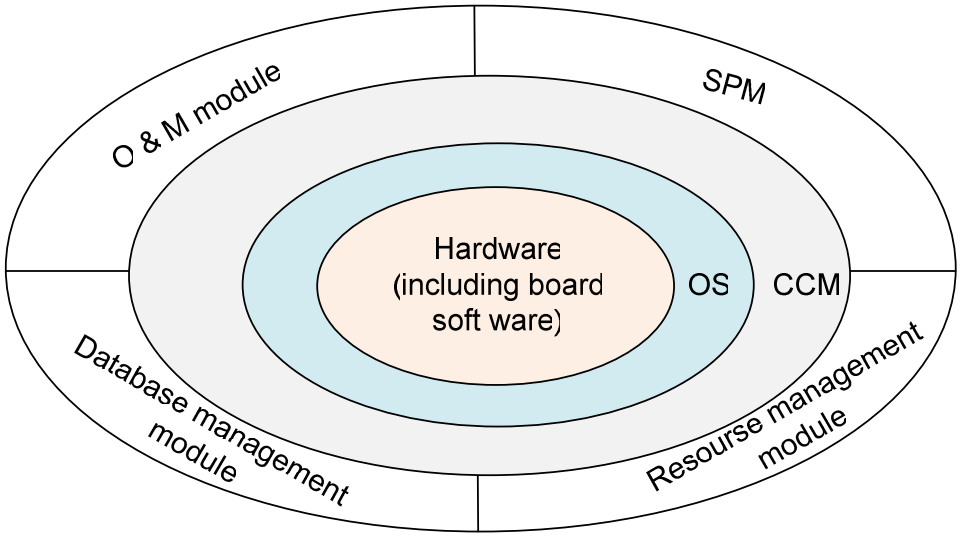

Рисунок 7.2 – Структура програмного забезпечення центру комутації рухомого зв'язку CDMA M800

Hardware (including board software) – це апаратні засоби з інтегрованим програмним забезпеченням; O&M module – це модуль експлуатації і технічного обслуговування; Database management module – це модуль управління базами даних; Resource management module – це модуль управління ресурсами.

CCM – модуль управління зв'язком управляє обміном даними між іншими модулями. Фізичним елементом, що реалізує цю функцію, є апаратний блок CCM.

SPM – модуль оброблення послуг – це ядро програмного забезпечення, що відповідає в M800 CDMA MSC за підтримку всіх послуг, що надаються абонентам системи. Даний програмний модуль здійснює

оброблення викликів, управління викликами й оброблення сигналізації. Фізичним елементом, що реалізує цю функцію, є модуль SPM.

Resource management module – модуль управління ресурсами здійснює управління спільними ресурсами, що глобально використовуються, включаючи з'єднувальні лінії, засоби передавання тональних сигналів, приймачі-передавач двотональних багаточастотних сигналів, приймачі-передавач MFC, накопичувачі EC і канали передавання даних. Фізичними елементами, що реалізовують ці функції, є SRM і плата CDP у модулі центрального процесора CPM.

Database management module – модуль управління базами даних, в основному, відповідає за управління базою даних з інформацією про користувачів. Фізичним елементом, що реалізовує цю функцію, є плата GVDP у модулі центрального процесора CPM.

O&M module (модуль експлуатації і технічного обслуговування) включає програми управління обладнанням і програми підтримки інтерфейсу технічного обслуговування. В даний програмний модуль надходить інформація про стан всіх плат та їх портів, стан процедур підтримки послуг на різних рівнях. Для виконання операцій технічного обслуговування модуль підтримує інтерфейс з BAM. Фізичним елементом, що реалізує цю функцію, є плата AMP у модулі центрального процесора CPM.

7.1.4 Надійність HUAWEI CDMA M800

Безперебійне живлення та відведення тепла від обладнання. Електроживлення обладнання ув системі здійснюється за допомогою розподілених джерел живлення, що гарантує високу ефективність використання електроенергії та стабільність напруги живлення. Полиці та функціональні модулі у стативах живляться від вторинних джерел живлення.

Всі вторинні джерела живлення у системі оснащені резервними напівкомплектами, що підвищує надійність системи електроживлення.

Для відведення надмірного тепла всі стативи системи оснащуються вентиляторами, по три зверху та знизу статива, що дозволяє організувати всередині статива примусову вентиляцію. Апаратні модулі iGWB і BAM вмонтовуються в одному стативі, в таких самих стативах встановлюються сервер, інверторне джерело живлення, комутатор LAN та інші пристрої. Всі вони є достатньо енергоємними пристроями, кожний такий модуль окремо оснащується своїм власним вентилятором. Відведення тепла від решти пристроїв здійснюється природним шляхом, тобто їх корпуси виконані таким чином, що забезпечується вільний доступ повітря ззовні у середину виробу.

Відмовостійкість апаратних засобів. Платформою для M800 CDMA MSC є цифровий комутатор «C&C08 Digital SPC Switch», що здійснює розподіл оброблення послуг. У даній платформі використовуються механізми багатократного резервування, сигналізація

про аварії та збої різних ступенів серйозності, гнучкі засоби локалізації збоїв і тестування обладнання. Ці механізми та засоби дозволяють досягти середнього часу напрацювання на відмову, що дорівнює 3623 дням.

Усі функції M800 CDMA MSC розподілені між різними функціональними модулями SPM, CCM, CPM, CNET і LIM. Ці функціональні модулі є незалежними один від одного й однозначно пов'язані з відповідними фізичними модулями, апаратними блоками та друкованими платами, що спрощує управління ними, виявлення й усунення несправностей, що в них виникають.

Усі друковані плати, що виконують найважливіші функції в M800 CDMA MSC, оснащені резервними напівкомплектами і можуть працювати або в режимі перерозподілу навантаження, або в режимі гарячого резерву. Кожна з цих плат у разі несправності може автоматично перемкнутися на резерв.

Мережа M800 CDMA MSC побудована на базі дубльованих субмереж, що працюють в режимі перерозподілу навантаження. В кожній з двох субмереж є модуль комутації (CCM), тобто будь-який, призначений для користувача, термінал може бути включений в мережу двома лінями HDLC, що належать обом дубльованим субмережам. Якщо обидві субмережі функціонують нормально, то зв'язок може здійснюватися або через субмережу № 0, або через субмережу № 1. Навантаження від всіх призначених для користувача терміналів динамічно розподіляється між двома субмережами, що працюють в режимі перерозподілу навантаження.

Всі плати системи підтримують функцію передачі звіту про версію апаратних засобів. Деяка плата може здійснювати завантаження програмного забезпечення без переривання функціонування. Вся плата оснащена флеш-пам'яттю. Запам'ятовуючі пристрої (ЗП), що містять програмне забезпечення плати, можуть бути перепрограмовані прямо на місці експлуатації, а деякі плати оснащені програмним забезпеченням, що дозволяє завантажувати оновлені програмні модулі без переривання функціонування. Тобто апаратні засоби системи можуть модифікуватися шляхом оновлення версії програмного забезпечення без заміни, власне, друкованої плати.

Надійність та безпека програмного забезпечення. Компанія HUAWEI отримала Сертифікат, що засвідчує відповідність її програмного забезпечення вимогам системи сертифікації CMM. Все програмне забезпечення M800 CDMA MSC було перевірено, протестовано, була встановлена його повна автентичність і завершеність. Таким чином, гарантується надійна та стабільна робота програмного забезпечення M800 CDMA MSC. Такі заходи як визначення критичного стану ресурсів, контроль за виконанням задач, захист збереженої інформації, перевірка даних і запис всіх виконуваних операцій дозволяють гарантувати стійке функціонування системи при виникненні незначних збоїв або помилок у виконуваних операціях.

Всі основні оперативні дані системи записуються в незалежні ЗК і періодично створюються резервні копії цих даних у модулях адміністрування високого і низького рівнів, тим самим гарантується цілісність даних.

Для підвищення надійності зберігання даних у деяких функціональних вузлах в MMU (модуль управління ЗК) може бути активізовано механізм захисту сегментів даних. (Після активізації цього механізму в MMU значно знижується продуктивність системи, тобто необхідно обрати такий режим захисту даних, за яких досягається оптимальне співвідношення між продуктивністю системи і цілісністю даних.)

Самодіагностика. Обладнання M800 CDMA MSC оснащено потужними засобами діагностики й автоматичного виявлення збоїв програмних і апаратних блоків, крім того, інформація про збої виводиться оператору і записується в ЗП. При збої апаратних засобів після виявлення несправного блока здійснюється його ізоляція або перехід на резервний напівкомплект. У разі збою програмного забезпечення система активізує засоби автоматичної корекції виниклих помилок і автоматичного відновлення нормального функціонування, включаючи перезапуск і перезавантаження. При виникненні серйозних збоїв крім повідомлення оператора і запису інформації в ЗП, активізується аварійна сигналізація. Після надходження у систему сигналу про збій апаратного блока система повторно здійснює процедуру пошуку місця виникнення несправності, і лише після підтвердження виниклого збою реєструє несправність. Така процедура захищає систему від виконання зайвих операцій її реконфігурування і зниження її продуктивності при випадкових збоях.

Для обладнання підтримки з'єднувальних ліній та сигнального обладнання у системі здійснюється тестування і локалізація збоїв з точністю до друкованої плати. Що стосується вузлів спільного управління, наприклад, модуль оброблення послуг, модуль мережної комутації, то у 70% випадків локалізація збою може бути виконана з точністю до однієї плати, в 90 % випадків – з точністю до двох плат (тобто можна визначити, що обидві плати або одна з двох несправні), у 100 % випадків – з точністю до трьох плат (тобто можна визначити, що з трьох плат несправні всі три плати, або дві, або одна з них).

Усі команди MML, виконання яких загрожує цілісності системи, вимагають введення підтвердження їх виконання.

Управління навантаженням системи. За умовчанням порогові величини навантаження ЦПУ, за якого активізуються процедури обмеження навантаження системи, дорівнює 80 %, а порогова величина, за якої знімаються обмеження навантаження системи, дорівнює 70 %. Відповідно до реальних умов роботи системи обслуговуючий персонал в центрі управління OMC може змінити ці значення порогів.

Для плавного регулювання трафіка M800 CDMA MSC необхідне, щоб порогова величина активізації обмежень була вища порогової

величини зняття обмежень. Тобто при виникненні перевантаження ЦПУ система знижує навантаження до тих пір, поки навантаження ЦПУ не впаде до нижнього порога. Така різниця порогових величин дозволяє уникнути частих запусків процедур обмеження навантаження системи.

M800 CDMA MSC дозволяє обмежувати трафік на різних інтерфейсах, включаючи A-інтерфейс і C/D-интерфейс та реалізовувати різнорівневі обмеження, наприклад на ділянці A-інтерфейсу трафік може знижуватися на 15 рівнів з плавним зменшенням розміру трафіка від 1 % до 100 %.

Обмеження навантаження на різних інтерфейсах реалізується шляхом заборони деяких послуг:

– A-інтерфейс: в основному, забороняються виклики всередині MSC MOC і MTC;

– C/D-интерфейс: забороняється оновлення даних місцеположення, додаткові послуги, передавання коротких повідомлень шляхом обмеження передачі MAP-повідомлень;

– TUP-интерфейс: забороняються вхідні виклики шляхом обмеження передачі TUP-повідомлень.

Засобом управління навантаженням на з'єднувальні лінії M800 CDMA MSC служить функція конфігурації пучків з'єднувальних ліній, тобто для кожного пучка можна задати кількість резервних ліній і портів. Якщо в якийсь момент кількість незайнятих портів стане менше числа резервного, то у системі автоматично запускається процедура обмеження навантаження. Але в цьому випадку у системі обмежуватимуться виклики звичних абонентів, а виклики абонентів з високим пріоритетом обмежуватися не будуть. Тобто в даному контексті термін «резервні порти» означає, що порти зарезервовані для обслуговування абонентів з високим пріоритетом.

Ця функція дозволяє гарантувати безперебійне обслуговування абонентів з високим пріоритетом в години найбільшого навантаження.

Початкові дані обліку вартості (білінгові дані), сформовані для кожного виклику, зберігаються в ЗП плати GSPC в M800 CDMA MSC. ЗП, призначений для зберігання цієї інформації, називається накопичувачем білінгової інформації. Початкові білінгові дані із ЗП плати передаються в iGWB, де тимчасово зберігаються і резервуються, а потім направляються в білінговий центр.

При виникненні збоїв (наприклад, при тимчасовому перериванні з'єднання між GSPC і iGWB) білінгові дані не можуть передаватися в накопичувач інформації в iGWB в реальному часі. Через деякий час при невідновленні збою накопичувач білінгових даних може бути переповнений (нові сформовані дані не можуть бути записані в ЗП при його переповнені), частина білінгових даних буде втрачена.

Щоб уникнути цієї ситуації у системі M800 CDMA MSC/VLR підтримується функція ієрархічного обмеження викликів. Тобто при заповненні накопичувача білінгових даних до певного рівня у системі

формується аварійний сигнал і активізується процедура обмеження викликів. А при повному заповненні накопичувача білінгових даних забороняються всі виклики.

Надійність та безпека системи обліку вартості послуг. Надійність системи обліку вартості послуг забезпечується такими заходами:

– живлення шлюзу iGWB здійснюється постійною напругою 48 В від двох дубльованих інверторних джерел живлення, один із яких є резервним. Така надмірна структура системи електроживлення гарантує безперебійну подачу напруги живлення;

– у системі використовується високоефективний промисловий сервер, дубльований резервним сервером такого ж класу;

– для забезпечення безперебійного зв'язку між хостом і iGWB всі фізичні лінії зв'язку дублюються, а також дублюються всі пристрої їхньої підтримки, тобто мережні адаптери і комутатори LAN;

– для коректного перемикання на резерв у разі збою між активним і резервним сервером 2 основні сполучні тракти також дублюються;

– конструкція й організація роботи дискових накопичувачів білінгових даних гарантує захист даних від помилок;

– білінгові дані записуються на два окремі диски Raid 5. При виході з ладу одного з дисків втрати даних не відбувається;

– матриця дискових накопичувачів оснащується одним резервним диском. При пошкодженні одного з дисків замість нього автоматично починає використовуватися резервний диск;

– iGWB може контролювати стан дисків і при виявленні збою активізує аварійну сигналізацію.

– у системі забезпечується контроль за станом виконуваних програмних процесів iGWB. При виявленні некоректного стану програмного процесу модуль контролю повідомляє в модуль загального управління про необхідність завершення або перезапуску цього процесу, або про необхідність переходу на резервне обладнання;

– для оперативного відновлення функціонування системи при виникненні збою iGWB миттєво передає аварійне повідомлення на панель аварійної сигналізації;

– у системі гарантується абсолютна цілісність білінгових даних, тобто білінгові дані не можуть бути загублені або помилково продубльовані.

Для забезпечення цілісності даних кожному пакету білінгових даних привласнюється унікальний порядковий номер. Шлюз iGWB приймає і записує пакети початкових білінгових даних з передаванням підтвердження в головний комп'ютер. У той самий час iGWB записує статус підтвердження білінгових даних з вказівкою ідентифікаторів прийнятих пакетів, за такої організації передавання пакетів жоден із них не може бути загублений або помилково продубльований. При виникненні збою на лінії зв'язку будь-який з пакетів може бути відновлений за його

порядковим номером, таким чином забезпечується повна ідентичність початкових білінгових даних і даних, що використовуються в білінговому центрі;

– шлюз iGWB періодично створює резервні копії найважливіших даних і здійснює перевірку коректності збережених даних. При виявленні помилок у даних, дані відновлюються за допомогою резервних копій. Завдяки періодичним перевіркам і резервуванням гарантується повна цілісність білінгових даних;

– для входу в програмне середовище білінгового клієнта користувачу необхідно увести свій обліковий запис, тобто ім.'я і пароль. Крім того, захист від неавторизованих операцій здійснюється таким чином: якщо протягом певного періоду часу користувач не виконав жодної операції, доступ до операцій забороняється, і поновлюється після повторного введення облікового запису;

– для захисту білінгових даних програмне середовище білінгового клієнта може бути конфігуровано тільки для виконання операцій з білінговими даними, реєстрації виконаних команд і аварійної сигналізації, можуть бути заборонені операції видалення і модифікації білінгових даних;

– шлюз iGWB оснащений мережними адаптерами, призначеними для роботи в різних сегментах мережі і функціонуючими незалежно один від одного. Повідомлення, передані через будь-який мережний адаптер, неприступні для інших адаптерів, таким чином, забезпечується розподіл доступу зовнішніх користувачів і користувачів внутрішніх мережних груп;

– у Web-сервері можна задати такі атрибути доступу за IP-адресою терміналу білінгового клієнта, щоб заборонити доступ до цих терміналів з неавторизованих мережних вузлів;

– щоб уникнути втрати білінгової інформації з моменту завершення виклику абонента до моменту передавання білінгової інформації в центр обліку вартості, білінгові дані піддаються чотирирівневій буферизації: буферизація в накопичувачі білінгових даних головного комп'ютера, буферизація файлів початкових білінгових даних, буферизація файлів оброблених білінгових даних, створення резервної копії даних на оптичному диску;

– місткість накопичувача білінгових даних головного комп'ютера дорівнює 64 Мбайтам, що дозволяє зберігати 330000 початкових рахунків;

– у iGWB після прийому з накопичувача початкових рахунків вони записуються на жорсткий диск (буферизація рівня 2);

– після оброблення початкових рахунків у білінговому сервері оброблені білінгові дані зберігаються на жорсткому диску (буферизація рівня 3), а потім прямують в центр обліку вартості;

– шлюз iGWB періодично створює резервні копії записаних на жорсткому диску білінгових даних, переносячи їх на магнітооптичний диск.

Захищеність програмних засобів вузла комутації була розлянута у розд. 5.6. Робота з персоналом, тобто кадрова безпека з профілактики витоку інформації була розглянута у п. 5.1.3. Деталі системи розмежування доступу на станції розкриті у розд. 5.7.

7.2 Інформаційна безпека ЦКС SI-2000

7.2.1 Загальна архітектура ЦКС SI-2000

Функціональна архітектура сімейства SI-2000 повною мірою відображає сучасні (на кінець XX століття) тенденції розвитку цифрових систем комутації та побудови мереж зв'язку. Вона повністю задовольняє рекомендаціям МСЕ-Т Q.511, Q.512 і базується на концепції універсального інтерфейсу для обладнання мережі доступу. Архітектурний розподіл вузла комутації (SN – Switch Node) та вузлів мережі доступу (AN – Access Node) різного функціонального призначення, дозволяє впроваджувати нові перспективні послуги електрозв'язку і сучасні технології абонентського доступу.

Реалізована незалежна від послуг архітектура мережі, яка об'єднує різні типи дротових і бездротових технологій доступу, технологій передавання по мідних (парних і коаксіальних) кабелях, волоконно-оптичних кабелях і радіозв'язку, а також може конфігуруватися й обслуговуватися єдиною системою управління. Застосовуються інтегровані в обладнання Si2000 сімейство установок електроживлення MPS (Modular Power Supply). Це дає можливість безпосередньо управляти первинними джерелами електроживлення персоналом станції.

У функціональній архітектурі сімейства SI-2000 передбачено вузол комутації і доступу (SAN – Switch and Access Node), що поєднує функції обладнання мережі доступу та комутованої мережі на базі одного апаратного модуля. Використання стандартного інтерфейсу V5.2 для підключення вузлів мережі доступу до вузла комутації дає можливість проводити централізоване управління абонентними даними як для обладнання, що входить до сімейства SI-2000, так і для обладнання вузлів мережі доступу сторонніх постачальників, що підтримує інтерфейси V5.1 та/або V5.2.

Наявність централізованої системи технічної експлуатації дозволяє управляти всіма вузлами сімейства SI-2000 з єдиного центру, що забезпечує значну економію експлуатаційних витрат оператора мережі зв'язку. Вузол управління (MN – Management Node) дозволяє проводити конфігурацію обладнання, моніторинг аварійних ситуацій, виконувати необхідні вимірювання параметрів якості обслуговування та навантаження. Сучасний діалоговий інтерфейс користувача на базі програмних засобів Windows NT полегшує оператору управління мережними елементами. Другою найважливішою функцією вузла управління є зберігання й оброблення станційних даних. Ці дані включають як контрольні копії завантажувального коду і бази напівпостійних станційних даних, так і дані

статистики, системного журналу, тарифікаційні дані тощо. Наявність програмного інтерфейсу, що задовольняє архітектурі і специфікаціям CORBA (Common Object Request Broker Architecture) забезпечує подальшу інтеграцію вузла управління в автоматизовану систему управління оператора мережі зв'язку (OSS – Operating Support System).

У сімействі SI-2000 реалізовано комп'ютерні вузли надання послуг (SVN – Service Node), що реалізують функції центрів оброблення викликів, довідкових систем, серверів доступу до ресурсів мереж передачі даних та інші застосування.

Апаратна платформа комутаційних вузлів сімейства SI2000 складається із багатофункціональних модулів. Це дозволяє створювати на базі одних і тих самих апаратних модулів різні мережні конфігурації, а також змінювати мережні функції системи комутації без заміни апаратного забезпечення шляхом перезавантаження напівпостійних станційних даних і частини програмного коду під управлінням вузла управління (MN). Апаратна платформа комутаційних вузлів сімейства SI-2000 включає наступні основні модулі:

MC (Module Central). Цей модуль є ядром комутаційної системи SI-2000. На його базі реалізуються вузли комутації для станцій великої та середньої ємності. Даний модуль також може використовуватися для побудови невеликих і середніх транзитних комутаційних вузлів різного функціонального призначення.

MLC (Module Line type C). Цей модуль використовується для побудови широкосмугових, вузькосмугових і комбінованих вузлів мережі доступу із застосуванням технологій SDSL і ATM, а також для побудови комутаційних станцій малої ємності як вузол комутації і доступу (SAN). Він може обслуговувати аналогові абонентні лінії, абонентні лінії базового доступу і доступу на первинній швидкості ЦМІС (Цифрових Мереж з Інтеграцією Служб).

Платформою MN є персональний комп'ютер, що за конфігурацією відповідає вимогам вузла управління (MN) для адміністрування заданого числа абонентів і мережних елементів. Найбільшою конфігурацією є багатопроцесорний сервер Windows NT для управління значною кількістю абонентів і комутаційних станцій з високим необхідним коефіцієнтом готовності. Однопроцесорний NT сервер використовується для управління однією або декількома комутаційними станціями і вузлами мережі доступу з порівняно невеликою сукупною абонентною ємністю. Робоча станція Windows NT використовується як клієнт MN для будь-якої зі згаданих вище конфігурацій сервера. Найменшою конфігурацією модуля MN є портативний комп'ютер типу «notebook» що використовує програмне забезпечення портативного термінала управління (MT), в якому одночасно працюють задачі сервера і клієнта програмного забезпечення MN.

Модульна установка електроживлення (Modular Power Supply – MPS). Сімейство MPS розроблене для забезпечення безперебійного електроживлення з напругою 48В або 60В і максимальним струмом 50А

(MPS 50), 140A (MPS 150) і 560 (MPS 500). MPS перетворюють початкову напругу для забезпечення необхідного навантаження і роботи акумуляторних батарей, на які передається обслуговування навантаження при порушеннях в мережі змінного струму.

Основними характеристиками MPS є:

– можливість дистанційного контролю й управління системою;

– захист від перенапруження по входу;

– захист батарей від глибокого розряду;

– активний розподіл навантаження по струму між випрямлячами;

– можливість заміни випрямлячів без виключення системи електроживлення;

– автоматичне термокомпенсування напруги заряду батарей;

– вимірювання симетрії акумуляторних батарей;

– можливість вимірювання реальної ємності акумуляторних батарей;

– індивідуальний заряд кожної акумуляторної батареї;

– управління струмом заряду акумуляторної батареї;

– генерація аварійних повідомлень при несправностях в обладнанні або критичних значеннях температури та передавання їх на вузол управління;

– можливість роботи з класичними або герметизованими батареями;

– запам’ятовування 400 останніх подій у системі живлення та навколишньому середовищі.

Система MPS має модульну архітектуру і, отже, розширення системи проводиться простим додаванням знімних блоків.

7.2.2 Платформа програмного забезпечення ЦКС SI-2000

Програмне забезпечення (ПЗ) в комутаційних вузлах SN/SAN підрозподіляється на системне ПЗ (System Software – SSW), прикладне ПЗ (Applications Software – ASW) та бази даних (Data Base – DB). Частиною системного програмного забезпечення є операційна система (Operating System – OS) на якій базуються інші підсистеми системного ПЗ (наприклад, SR3, OLT, ODOLT) і прикладне програмне забезпечення.

Системне програмне забезпечення комутаційних вузлів сімейства SI-2000 включає операційну систему (OS), підсистему початкового завантаження і відновлення (Start-up_Reliability_Resiliency_Recovery – SR3), підсистему фонового тестування (On-Line Tests – OLT) і підсистему тестування за запитом (On-Demand On-Line tests – ODOLT). Операційна система (pSOS+) складається з ядра і системних програм стека протоколів TCP/IP та його застосувань. В ній реалізовані протоколи для передавання аварійної індикації та даних про помилки (в даному випадку – SNMP), передавання програмних файлів станційного ПЗ, інформації обліку вартості та статистики тощо (в даному випадку FTP) і для виконання процедур адміністрування (в даному випадку RPC). Маршрутизатор IP для забезпечення зв’язку з вузлами реалізовано в комутаційному вузлі (SN/SAN).

Прикладне програмне забезпечення комутаційних вузлів сімейства SI-2000 включає програми оброблення сигналізації (Signaling Processing – SP), управління викликом (Call Control – CC), управління додатковими послугами (Supplementary Services – SSV), обліку вартості та реєстрації (Call Registration and Charging – CRC), управління мережними з'єднаннями (Connectivity and Senders Control – CSC), вимірювань і статистики (Traffic and Statistical Measurements – TSM).

Бази даних SI2000 (DB). Вузол управління (MN) містить СУБД «Informix DBMS (On-line)», тоді як комутаційні вузли SN/SAN містять СУБД «SI2000 Real Time DataBase Management System (RTDBMS)». Обидві СУБД є релятивістськими. Бази даних можуть адмініструватися за допомогою інтерактивної графічної мови Informix NewEra.

7.2.3 Забезпечення безпеки ЦКС SI-2000

Безпека телекомунікаційної системи забезпечується за допомогою відповідних заходів захисту. Політика безпеки системи повинна бути визначена документом, в якому описуються способи і процедури, що запобігають зловживанням і неправильному поводженню з системою. Проведенням цієї політики забезпечується оптимальний рівень безпеки відповідно до вимог. Різні рівні безпеки системи досягаються застосуванням захисних заходів різних рівнів.

Присвоєння категорій користувачам. Категорією користувача визначається основна область діяльності користувача. Користувач повинен бути включений щонайменше в одну з наступних категорій:

– категорія NT System – користувач Windows NT;

– категорія MN – адміністрування з використанням застосувань MN;

– категорії TRANSFER і CENTREX – дистанційний доступ до тарифних даних.

У категорію NT System включаються всі користувачі категорій MN, TRANSFER і CENTREX.

До категорії MN можуть відноситися всі користувачі, що мають основний доступ до діяльності з управління категорії MN – члени групи MN_USERS. Дозвіл на роботу із застосуваннями дається користувачам залежно від типу застосування та виду виконуваної роботи (перегляд даних або зміна і переглядання даних). Управління безпекою користувачів категорії MN виконується за допомогою групи команд Permissions.

Користувачі категорії TRANSFER – це всі користувачі, що мають основний доступ до діяльності з управління категорії TRANSFER – члени групи TRANSFER_USERS. Дозвіл на роботу із застосуваннями визначається членством користувача в групі Windows. Управління безпекою користувачів категорії TRANSFER виконується в групі команд Group Manager.

Користувачі категорії CENTREX – це всі користувачі, що мають основний доступ до діяльності з управління категорії CENTREX – члени

групи CENTREX_USERS. Дозвіл на роботу із застосуваннями визначається членством користувача в групі Windows NT. Управління безпекою користувачів категорії CENTREX виконується в групі команд Group Manager.

Група MN. Користувач застосувань MN може бути включений в одну або декілька груп MN, залежних від продукту: AmgUsers, AmgAdmins, CmgUsers, CmgAdmins, FmgUsers, FmgAdmins, PmgUsers, PmgAdmins, SmgUser, SmgAdmins, SysUsers, SysAdmins.

Перші три літери дозволу визначають застосування MN. Групи xxxUsers дозволяють переглядати (прочитувати) дані в застосуваннях, а групи xxxAdmins – змінювати та переглядати дані.

Доступ до MN. Доступ до MN захищений дозволами, що є складовою частиною Windows NT. При входженні у систему користувач ідентифікує себе за допомогою імені користувача і пароля. Якщо вхід у систему був успішний, користувач отримує доступ до загальних застосувань в MN.

Якщо користувач якийсь час не працює активно із застосуванням MN, активізується хранитель екрана. Для подальшої роботи із застосуванням MN необхідна ідентифікація користувача.

Доступ до застосувань MN. Доступ до застосувань визначено категорією користувача та групою MN. Застосування «Управління безпекою – SMG» забезпечує додатково захист зміни або перегляд даних окремого вузла, груп команд, а також захист доступу до окремих даних.

Застосування «CMG» поділяється на декілька груп, команд (наприклад: Subscriber (абонент), Routing (маршрутизація) тощо), а група команд в решті застосувань MN («AMG», «FMG»,...) незмінна. Адміністрування дозволів користувачів на роботу з групами команд описано у вікні Group Commands. Застосування дозволяє також обмежити доступ користувачів до окремих даних. Для користувача можна адмініструвати декілька обмежувальних інтервалів. Якщо для користувача в даних не записаний ніякий інтервал, такий користувач має необмежений доступ до всіх значень даних. Адміністрування виконується у вікні Accessible Range.

Тип користувача. Користувачі застосування «Управління безпекою – SMG» розподілені на чотири типи:

– користувач з дозволом sysadmin, що має право на користування всіма застосуваннями («AMG», «CMG»,...), є єдиним користувачем, який може виконувати всі процедури управління безпекою застосування «SMG»;

– користувач з дозволом SMG – Read/Write, що адмініструє дозволи на доступ решти користувачів до вузлів і дозволи на адміністрування груп команд;

– користувач з дозволом SMG – Read/Only, який може лише переглядати, які дозволи мають користувачі на доступ до вузлів і груп команд;

– користувачі застосувань MN, які не можуть виконувати запуск застосування «SMG».

Захист передавання тарифних даних в обчислювальний центр розрахунку з абонентами. Дистанційний доступ до спільних тарифних даних здійснюється з використанням стандартного протоколу FTP для потреб обчислювального центру розрахунку з абонентами і захищений за допомогою імені користувача і пароля. Центр розрахунку з абонентами має доступ до тарифних даних тільки в рамках тих дозволів, які йому були дані адміністратором в групі команд Group Manager.

Захист передавання тарифних даних бізнес-груп. Дистанційний доступ до тарифних даних бізнес-груп, що здійснюється за допомогою стандартного протоколу FTP, має захист за ім'ям користувача і паролем. Доступ адмініструється окремо для кожної бізнес-групи. Захист даних нових бізнес-груп виконується програмно при формуванні кожної окремої групи. Адміністрування дозволу на доступ до даних бізнес групи виконується в групі команд Group Manager.

7.3 Парольний захист

Перелік загроз для цифрових АТС, що реалізуються шляхом злому парольного захисту:

– загроза атаки через робоче місце станційного інженера (термінал);

– загроза несанкціонованого входу в термінал управління мережею оператора, АТС;

– загроза модифікації системного або програмного забезпечення адміністрування вузла зв'язку.

– загроза зараження файлів комп'ютерними вірусами.

Правила формування пароля. Персональні паролі повинні генеруватися спеціальними програмними засобами або обиратися персоналом самостійно з урахуванням наступних вимог:

– довжина пароля повинна бути не менше 8 символів, оптимальний варіант – 12–14 символів. Збільшення пароля усього на два символи дає в 500 разів більше варіантів, ніж збільшення алфавіта на 18 символів;

– у складі символів пароля обов'язково повинні бути присутніми літери верхнього та нижнього регістрів, цифри та спеціальні символи (" ~ ! @ # $ % ^ & * ( ) – + _ = \ | / ?,);

– при зміні пароля нове значення повинне відрізнятися від попереднього не менше ніж в 4 (5, ..., 7, 8) позиціях;

– особистий пароль користувач не має права повідомляти нікому;

– пароль не повинен включати легко обчислювані поєднання символів (імена, прізвища, відомі назви, словарні та жаргонні слова тощо), послідовності символів і знаків (111, qwerty, abcd тощо), загальноприйняті скорочення (ЕОМ, ЛВС, USER і т.п.), абревіатури, клички домашніх тварин, номери автомобілів, телефонів та інші значущі поєднання літер і знаків, які можна вгадати, ґрунтуючись на інформації про користувача.

Введення пароля. При введенні пароля користувачу необхідно виключити можливість його підглядання сторонніми особами (людина за спиною, спостереження людиною за рухом пальців у прямій видимості або у відбитому світлі) та технічними засобами (стаціонарними і вбудованими в мобільні телефони відеокамерами тощо).

Порядок зміни особистих паролів. Зміна паролів повинна проводиться регулярно, не рідше одного разу на два місяці (або вказати точний інтервал у днях). У разі припинення повноважень користувача (звільнення або переходу на іншу роботу) проводиться негайне видалення відразу після закінчення його останнього робочого дня.

Термінова (позапланова) повна зміна паролів повинна проводиться у разі припинення повноважень (звільнення або переходу на іншу роботу) адміністраторів інформаційної системи й інших співробітників, яким за родом роботи були надані повноваження з управління системою парольного захисту.

Необхідно вести «Журнал примусової зміни особистих паролів», в якому наголошується на причинах позапланової зміни паролів користувачів.

Зберігання пароля. Забороняється записувати паролі на папері, у файлі, електронному записнику й інших носіях інформації, зокрема на предметах.

Забороняється повідомляти іншим користувачам особистий пароль і реєструвати його у системі під своїм паролем.

Зберігання користувачем свого пароля на паперовому носії допускається лише в особистому, опечатаному власником пароля сейфі, або у сейфі у відповідального адміністратора [системи парольного захисту], або керівника підрозділу в опечатаному особистою печаткою пеналі.

Власники паролів повинні бути ознайомлені під розпис з перерахованими вище вимогами та попереджені про відповідальність за використання паролів, що не відповідають даним вимогам, а також за розголошування парольної інформації.

7.4 Формування позасистемних складових КСЗІ на ЦАТС

Наведемо приклад формування комплексної системи захисту від витоку інформації системами електроживлення, заземлення, вентиляції, пожежної сигналізації та засобів фізичного захисту інформації.

7.4.1 Загальні відомості щодо об’єкта

У даному випадку розглядається приміщення опорного вузла зв’язку оператора мобільного зв’язку. Приміщення розташовані на другому поверсі чотириповерхової будівлі. Кількість приміщень – 3: автозал, кімната персоналу, коридор. Захищаючі приміщення стіни виконані з керамічної обпаленої цеглини, а внутрішні перегородки з гіпсокартонових листів, що кріпляться до металевого профілю. Приміщення опорного вузла

необхідно обладнати комплексною системою захисту інформації. Для вибору засобів захисту інформації від витоку необхідно мати уявлення про склад комунікаційних споруд об'єкта, а саме систем електроживлення, заземлення, вентиляції, пожежної сигналізації. Дані схеми наведені на рис. 7.3...7.6.

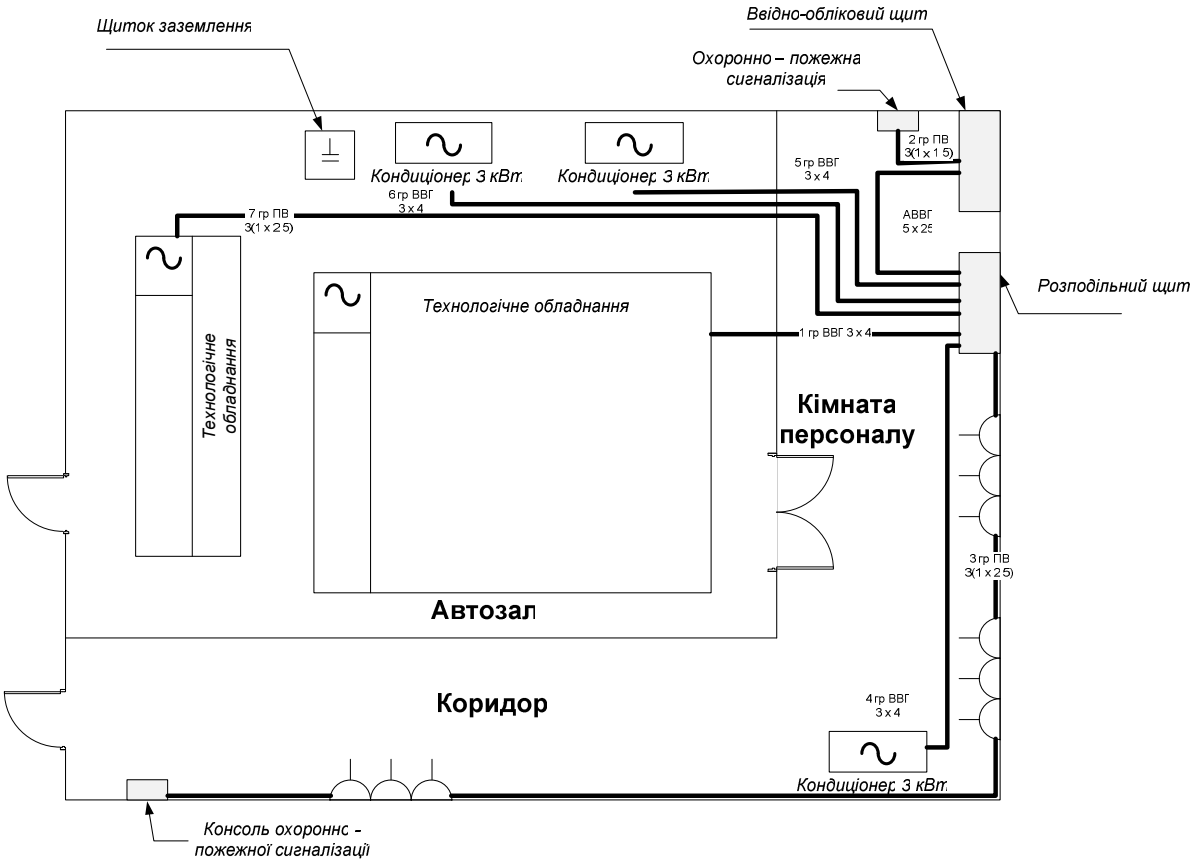

Рисунок 7.3 – Система електроживлення

У приміщенні кімнати персоналу встановлено ввідно-обліковий ящик з електричним лічильником 380В/50 Гц на 25 кВт. На зовнішній стіні встановлено герметичний рознім типу 5П32А (ШР20П5) для підключення дизель-генератора. Для перемикання типу живлення від основного до резервного передбачено перекидний розмикач. Виконано окремий контур заземлення. План контуру заземлення показано на рис. 7.4.

Для виявлення пожежі в приміщеннях, що захищаються, встановлені автоматичні димові пожежні сповіщувачі СПД 3.1 і ручні пожежні сповіщувачі ІПР « Алай - 2 - 01» (рис. 7.5).

Для прийому сигналів про спрацьовування сповіщувачів передбачено приймально-контрольний прилад «Гамма - 104». Для індикації сигналів про пожежу передбачений оповісник ОПОК 4 - 1.

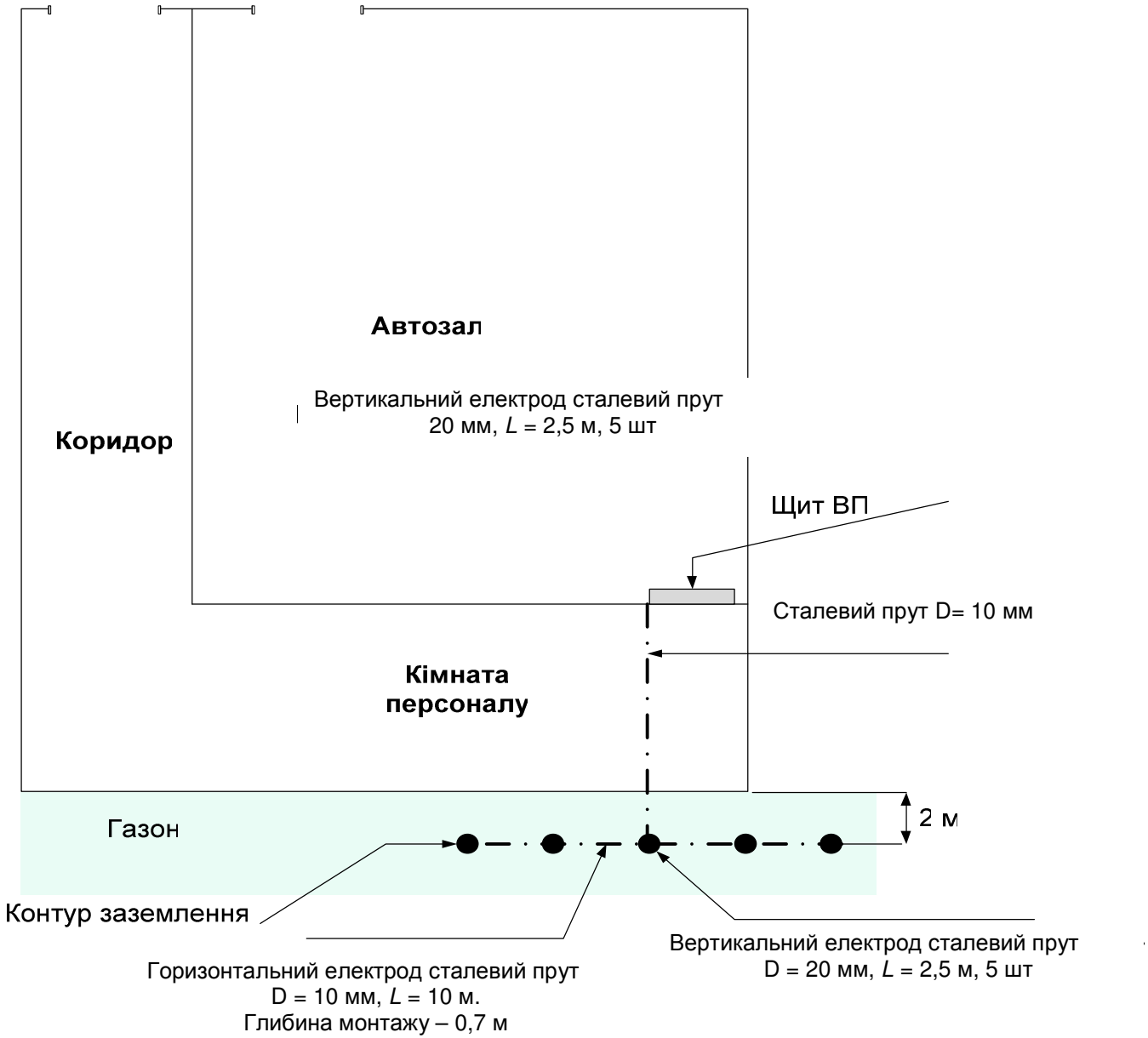

Рисунок 7.4 – План контуру заземлення

Передбачено виведення дублюючого сигналу про пожежу на ПЦС УДПО відповідно до п. 1.1.7 ДБН В.2.5 – 13 – 98. Виведення дублюючого сигналу здійснюється відповідно до укладеного договору з ПЦС УДПО.

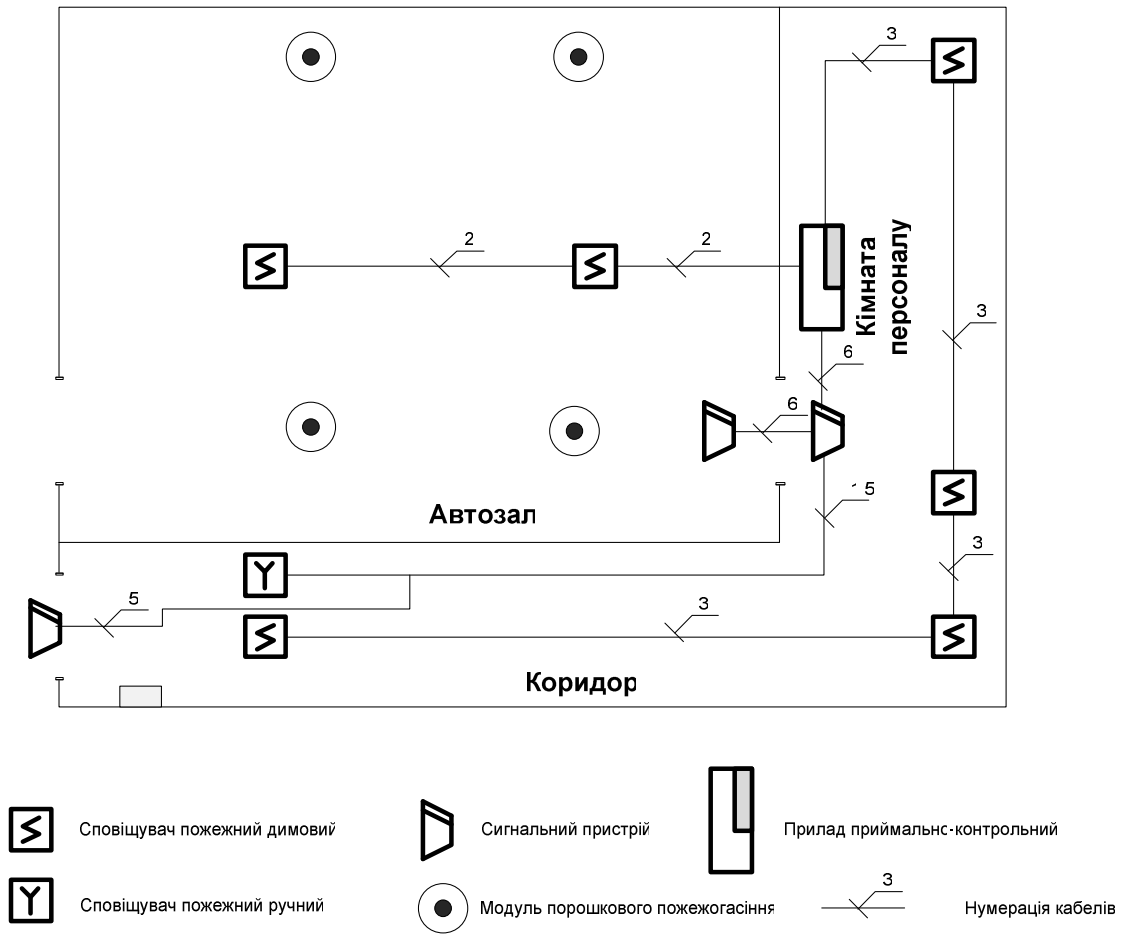

Рисунок 7.5 – Система пожежної сигналізації

Передбачене установлення в приміщенні автозалу модулів порошкового пожежегасіння, що автоматично спрацьовують при підвищенні температури вище нормативних показників. Система забезпечує прийом сигналів про пожежу та пошкодження і передбачає акустичний та оптичний сигнали про небезпечні події.

Для примусового відключення вентиляції при пожежі передбачено контакти реле, що керуються приймально-контрольним приладом.

Кондиціонування приміщень автозалу і кімнати персоналу здійснюється за допомогою двох промислових кондиціонерів LG – 24 S – LHP (автозал) і промислового кондиціонера LG – 3 – 9 – LHV. Передбачено підключення автоматики кондиціонерів до системи автоматичного пожежогасіння для автоматичного виключення при спрацьовуванні датчиків пожежної сигналізації (рис. 7.6).

Оскільки в приміщенні автозалу встановлені герметичні акумулятори, то згідно вимог по експлуатації герметичних акумуляторів необхідно забезпечити провітрювання приміщення з попаданням

зовнішнього повітря в нижню зону приміщення, а видалення внутрішнього повітря з верхньої зони приміщення. Тому приміщення опорного вузла обладнані системою проточно-витяжної вентиляції.

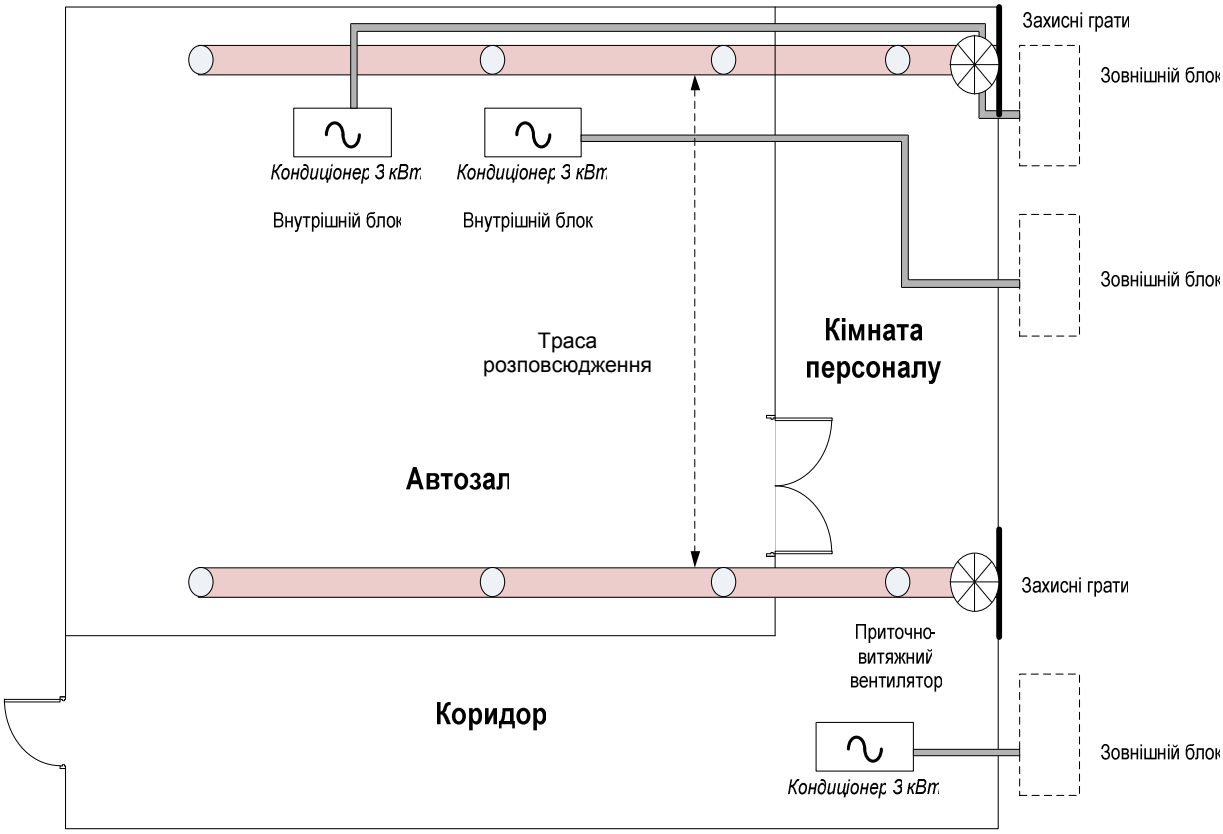

Рисунок 7.6 – Система вентиляції та кондиціонування

Також передбачено автоматичне відключення вентиляторів при спрацьовуванні датчиків пожежогасіння.

7.4.2 Фізичний захист інформації

Система відеоспостереження. Система відеоспостереження побудована з використанням зарубіжного обладнання на базі дуплексного мультиплексора з вбудованим детектором руху MV16p.

Оскільки на опорному вузлі зв'язку існує цілодобове чергування з метою моніторингу стану системи зв'язку оператора, і своєчасного виявлення та усунення нештатних ситуацій на мережі, то контроль і управління системою відеоспостереження здійснюватиметься силами чергової зміни.

У кімнаті персоналу встановлені:

– дуплексний мультиплексор MV16p;

– два накопичувача AG-TL 700 (для постійного відеоархівного запису та відтворення);

– два монітори (головний монітор 19″ WV-BM 1900 і другий монітор 17″ WV-BM 1700);

– джерело живлення для внутрішніх відеокамер ALTV 1224.

Мультиплексор має вбудований детектор руху для внутрішніх відеокамер, входи тривоги по кожному каналу і вбудований індикатор пропадання відеосигналу. Детектування здійснюється за трьома параметрами: чутливість, розмір об'єкта та тривалість руху. Наявність двох режимів роботи (день / ніч) дозволяє автоматизувати процес взяття під охорону.

План мережі відеоспостереження показано на рис. 7.7

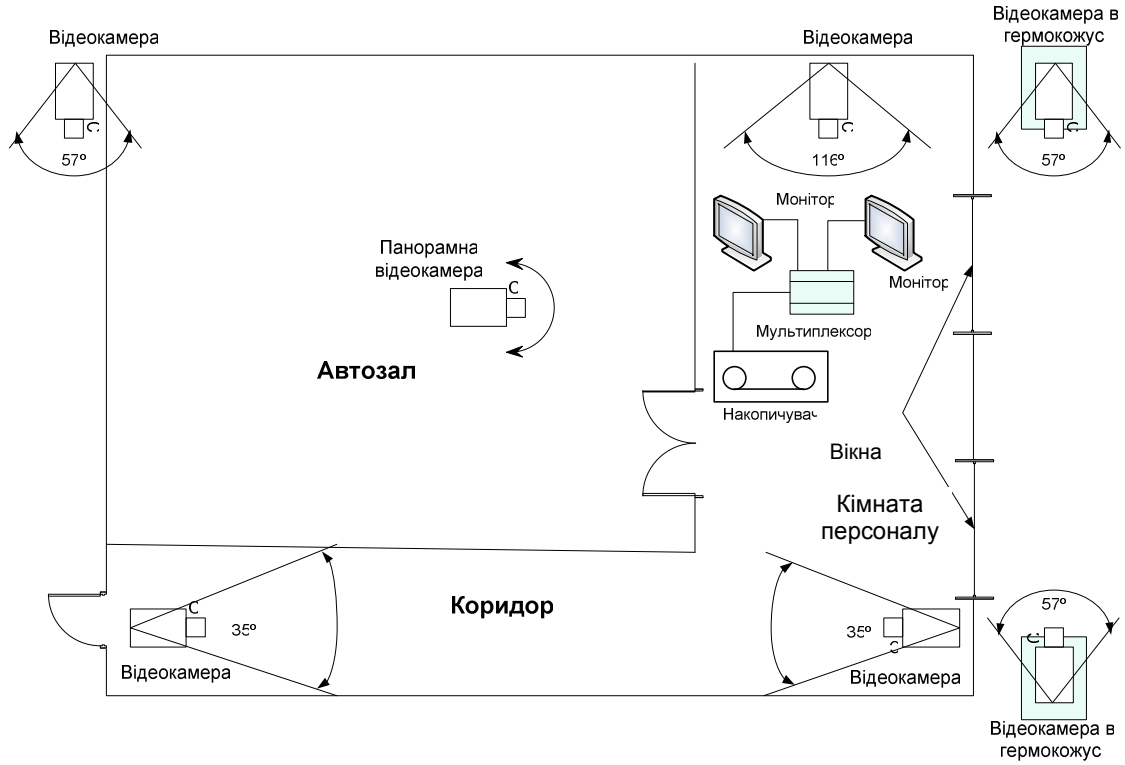

Рисунок 7.7 – План мережі відеоспостереження

Технічні засоби відеспостереження забезпечують:

– ручне управління елементами системи відеоспостереження;

– цілодобове спостереження як за внутрішніми приміщеннями вузла, так і за суміжним коридором і ділянкою простору, що примикає до зовнішньої стінки приміщення вузла;

– переглядання зображень від будь-якої телекамери за допомогою моніторів, розташованих в кімнаті персоналу;

– цілодобовий запис зображень від усіх відеокамер з реєстрацією часу, дати і номера відеокамери;

– розширення системи до 16-ти телекамер;

– відтворення запису для перегляду.

Структурна схема мережі телевізійного спостереження (CCTV) показана на рис.7.8.

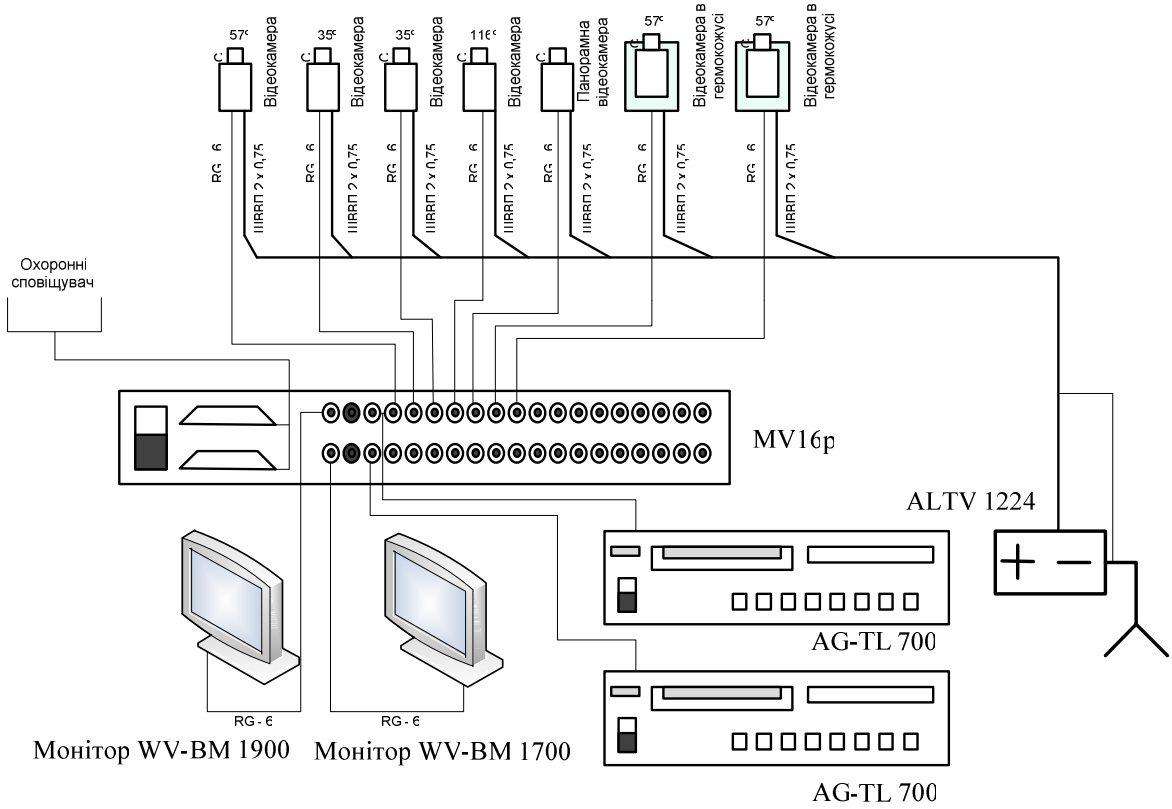

Рисунок 7.8 – Структурна схема мережі телевізійного спостереження

Вище наведено один із варіантів формування системи охоронного телебачення, що використовує аналогову технологію (CCTV). В даний час, враховуючи розвиток техніки та все більш помітну інтеграцію в мережеві аспекти, проектувальники та інженери володіють досить великими можливостями при побудові систем відеоспостереження. Враховуючи обширність питання, хочеться відзначити використання гібридних технологій (з використанням відеокодерів), що дозволяють об'єднувати аналогові ділянки систем відеоспостереження з існуючими цифровими областями, а також, безсумнівно, IP-системи. Структурна схема реалізації гібридної системи наведена на рис. 7.9. Динаміка розвитку і застосування IP-систем викликана все більшою інтеграцією підсистем фізичної безпеки в єдину, комплексну систему, а також розвитком бездротових мереж і доступною ціною каналів зв'язку.

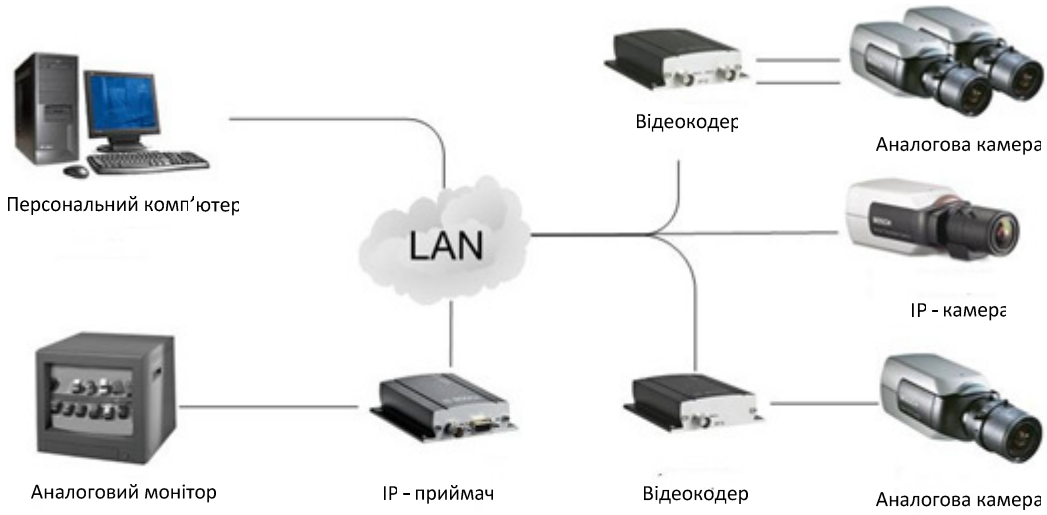

Рисунок 7.9 – Структурна схема реалізації гібридної системи відеоспостереження

Контроль доступу. Контроль доступу – одна з частин системи комплексної безпеки об'єкта. Сучасні системи контролю доступу (СКД) за своїми можливостями можуть забезпечити будь-який рівень охорони на об'єктах, що містять тисячі точок доступу та десятки тисяч користувачів.

Системи контролю доступу – це основа для побудови системи фізичної безпеки, що об'єднує охоронну, пожежну сигналізацію та систему відеоспостереження.

За способом управління системою, СКД можна класифікувати таким чином:

– автономні (локальні) – для управління одним або декількома пристроями, перекриваючими, без передавання інформації на центральний пульт і без контролю з боку оператора;

– централізовані (мережні) – для управління перекриваючими пристроями з обміном інформацією з центральним пультом, контролем і управлінням системою з боку оператора;

– універсальні, що включають функції як автономних, так і мережних систем, які працюють у мережному режимі під керівництвом центрального пристрою управління та переходять в автономний режим при виникненні відмов у мережному обладнанні або центральному пристрої.

Через те що, приміщення вузла зв'язку обладнано лише одними вхідними дверима, то достатньо встановити локальну СКД (рис. 7.10).

Така система складається з автономного контролера, що зберігає у собі базу даних ідентифікаторів й управляючого роботою решти елементів системи. Як виконавчий пристрій використовується електромагнітний замок, або кнопка. Для ідентифікації користувача використовуються різні проксиміті карти з відповідними зчитувачами.

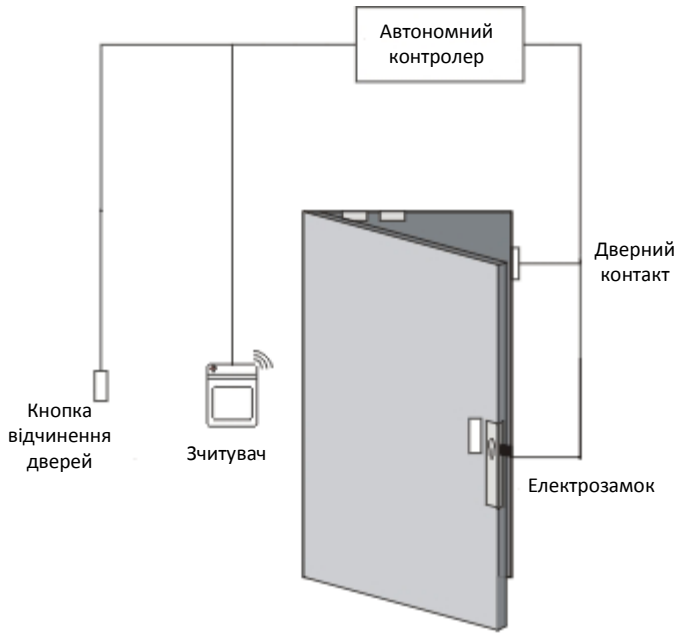

Рисунок 7.10 – Структурна схема автономної СКД

Контролер працює, як правило, з одним зчитувачем на вхід, для відкриття замка з середини приміщення звичайно використовується кнопка. Типовим прикладом автономного контролера є контролер МД64, що забезпечує роботу з одним зчитувачем проксиміті картки або Touch Memory зчитувачем, який дозволяє забезпечити автономний контроль за доступом в окреме приміщення. Технічні характеристики контролера МД64 показані в табл. 7.1.

Таблиця 7.1 – Технічні характеристики контролера МД64

Основні характеристики	
Тип:	КОНТРОЛЕР
Формат карт:	Proximity та Touch Memory
Максимальна кількість ключів:	63+1 майстер
Число можливих комбінацій:	280 трильйонів
Кількість комутованих виходів:	1
Електричні параметри	
Напруга живлення:	12–14 В
Струм споживання в черговому режимі:	35 мА
Струм комутації реле:	10 А
Допустима довжина кабелю до зчитувача:	25 м
Найменування за каталогом:	Контролер МД64
Інші назви:	МД 64, МД–64, MD64, MD–64, MD 64
Габаритні розміри:	55х43х20 мм
Гарантія:	12 міс.

Крім того, вхід в будівлю, де знаходяться приміщення вузла зв’язку, здійснюється за пропусками встановленого зразка.

Охоронна сигналізація. Задача охоронної сигналізації (ОС) – захистити приміщення від несанкціонованого проникнення сторонніх осіб. Умовно охоронні сигналізації можна поділити на два типи:

Автономна система ОС. У разі спрацьовування такої системи активуються сирени, строб-спалахи тощо. Сигнал тривоги нікуди не передається.

Сигналізація з підключенням до пульта централізованого спостереження (ПЦС), так звана пультова охорона. Захист приміщень здійснюється шляхом установки в них охоронних сповіщувачів (датчиків). Сучасні системи охоронної сигналізації можуть бути оснащені наступним додатковим обладнанням: блоком голосового телефонного дозвонщика, який у разі тривоги передає по телефонній лінії (у разі її наявності) наперед записане голосове повідомлення на запрограмовані телефонні номери; GSM-модулем, що дозволяє передавати повідомлення про тривогу. Спеціальними сервісними датчиками, що відстежують витік побутового газу або протікання води.

Це обладнання підключається до контрольної панелі охоронної сигналізації – «мозку» системи, який являє собою друковану плату з клемами, розташовану в металевому боксі. Також до контрольної панелі підключаються клавіатура, за допомогою якої здійснюється поставлення і зняття з охорони, оповісники (сирени, строб-спалах тощо) та всі додаткові елементи.

У класичному вигляді підключення здійснюється за допомогою дротів, тобто до кожного складового елементу охоронної сигналізації (датчика, клавіатури, сирени тощо) повинен бути прокладений дріт від контрольної панелі. Останнім часом все більшу популярність завойовують бездротові елементи, що підключаються до контрольної панелі по радіоканалу.

Будь-яка технічна система безпеки повинна мати безперебійне живлення всіх своїх складових частин. Класична охоронна система складається з наступних елементів: контрольної панелі, пристроїв управління (клавіатур тощо), сигнальних пристроїв (сирен тощо), датчиків. Система охоронної сигналізації побудована на основі приймально-контрольного приладу «Лунь-7Т». Зовнішній вигляд пристрою показано на рис. 7.11.

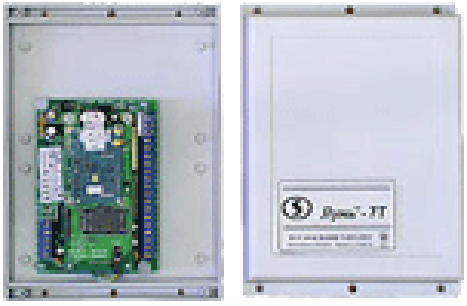

Рисунок 7.11 – Зовнішній вигляд ППК «Лунь-7Т»

Характеристики ППК «Лунь-7Т»:

– кількість шлейфів з кінцевим резистором і контролем опору: 8;

– можливість розширення за допомогою ППК «Лунь-7Н», кожен прилад – окрема група шлейфів, до 30 шт.;

– кількість електронних ключів: 15;

– пам’ять подій: 64;

– типи підтримуваних шлейфів – звичний охоронний, вхідний (затриманий), прохідний (внутрішній – з затримкою), 24-годинний. Будь-який зі шлейфів може бути ще і тихим (при порушенні не включається сирена). Типи шлейфів виставляються програмою «Конфігуратор»;

– опір кінцевого резистора: 4,7 кОм;

– напруга живлення від джерела безперебійного живлення: 10-14 В;

– контроль 220 В і АКБ;

– передавання тривожної інформації на ПЦС голосовим каналом стільникового зв’язку стандарту GSM 900/1800 або GPRS GSM 900/1800.

Схема розміщення системи охоронної сигналізації на об’єкті показана на рис. 7.12.

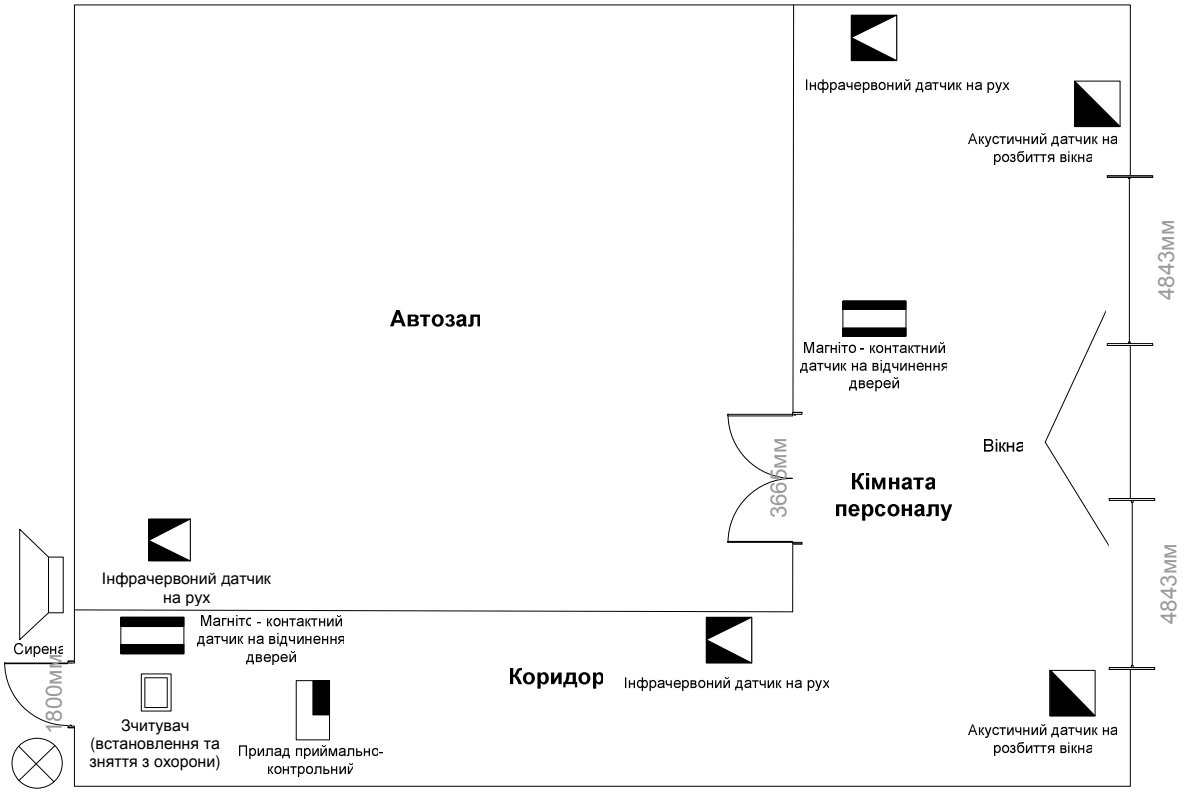

Рисунок 7.12 – Схема системи охоронної сигналізації

Подібна система має декілька кордонів охорони, що ефективно захищають всі вікна та двері. Призначена для запобігання проникненню в приміщення і розкрадання (псування) майна.

Система з передаванням сигналу на пульт централізованої охорони. При проникненні – миттєво на місце прибуває мобільна група і затримує зловмисників.

7.4.3 Захист засобів оброблення та реєстрації інформації від витоку ланцюгами електроживлення та заземлення

З метою захисту засобів оброблення та реєстрації інформації використовуються фільтри мережні завадопоглинаючі типу ФСП-1. Фільтри мережні завадопоглинаючі типу ФСП-1 призначені для:

– захисту засобів оброблення та реєстрації інформації від витоку ланцюгами електроживлення та заземлення;

– захисту засобів оброблення та реєстрації інформації від високочастотних мережних перешкод.

Фільтри сертифіковані та включені в перелік засобів загального призначення, які дозволено застосовувати для забезпечення технічного захисту інформації.

Технічні дані:

– номінальна напруга, 250 В;

– номінальна частота напруги і струму, 50 Гц;

– номінальний струм, 20 А;

– загасання несиметричних перешкод, що вноситься на частотах від 0,1 МГц до 1 000 МГц, не менше 60 дБ.

Розміри корпусу фільтра: 430 × 150 × 80, мм. Маса: не більше 5,5 кг.

Питання для самоконтролю

1. Дайте коротку характеристику архітектури центру комутації рухомого зв’язку HUAWEI CDMA M800.
2. Поясніть архітектуру програмного забезпечення центру комутації HUAWEI CDMA M800.
3. Які функції інформаційної безпеки обладнання HUAWEI CDMA M800?
4. Як забезпечується захищеність програмного забезпечення центру комутації HUAWEI CDMA M800?
5. Поясніть принипи роботи з персоналом на ЦАТС.
6. Поясніть архітектуру ЦКС SI-2000.
7. Як захищається передача тарифних даних в ЦКС SI-2000?
8. Сформулюйте принципи вибору, вводу та зберігання паролю.
9. Опишіть способи захисту інформації від витоку ланцюгами живлення та заземлення.
10. Які підсистеми можуть входити до складу системи фізичного захисту?
11. Основні задачі та варіанти побудови систем охоронної сигналізації.
12. Які технології можуть використовуються при побудові систем відеоспостереження?
13. Наведіть базовий склад типової системи відеоспостереження.

8 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.

Значну допомогу у написанні цього розділу, створенні методик оцінки витрат на інформаційну безпеку ЦАТС та проведенні розрахунків було надано кандидатом економічних наук Т.М. Тардаскіною.

8.1 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 установленого порядку маршрутизації інформації.

Необхідний рівень безпеки можна визначити за 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, втратою 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 обладнання;

– витрати на організацію мережної взаємодії і безпечного використання ЦАТС;

– витрати на підтримку системи резервного копіювання і ведення архіву даних;

– проведення інженерно-технічних робіт з встановлення сигналізації, обладнанню 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 за підрозділами;

– оплата робіт з контролю правильності введення даних у прикладні системи;

– оплата інспекторів з 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 у 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 переоцінки 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 та інших інформаційних масивів;

– витрати на проведення заходів щодо контролю вірогідності даних, які піддавалися атаці на цілісність;

3) витрати на виявлення причин порушення політики безпеки:

– витрати на проведення розслідувань порушень політики безпеки (збирання 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 суттєвої 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;

– відмова від організаційних, науково-технічних чи комерційних рішень, що стали неефективними в результаті витоку відомостей, 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 обладнанні технологій, у тому числі підвищенні цін на них;

4) економічний збиток:

– інші види можливого збитку підприємству, у тому числі пов’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.

8.2 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 надто 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 межі 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.

8.2.1 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 взаємопов’язаних і взаємозалежних компонентів. Оцінка ступеня захищеності окремих телекомунікаційних об’єктів – вузлів, станцій, маршрутизаторів, серверів – є складною задачею, яка виконується експертами.

Дослідження в області експертних систем показали ефективність застосування для розв’язання 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 в експертній системі підтримки прийняття рішень з оцінки варіантів розподілу механізмів інформаційної безпеки з використанням нечіткої логіки та нечітких множин, можна запропонувати мережну конструкцію, яка задається у вигляді

$$C = <X_{11},\ldots, X_{ij}; R_1,\ldots, R_k; G>, \quad (8.1)$$

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;

$R_1,\ldots, R_i$ – 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, в якій розглядається взаємодія між об'єктами (рис. 8.1).

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 рішення. Кожне правило базується на інформації, отримуваної від експерта. За допомогою правил рішення проводиться часткове впорядкування (ранжирування) точок простору вхідних показників.

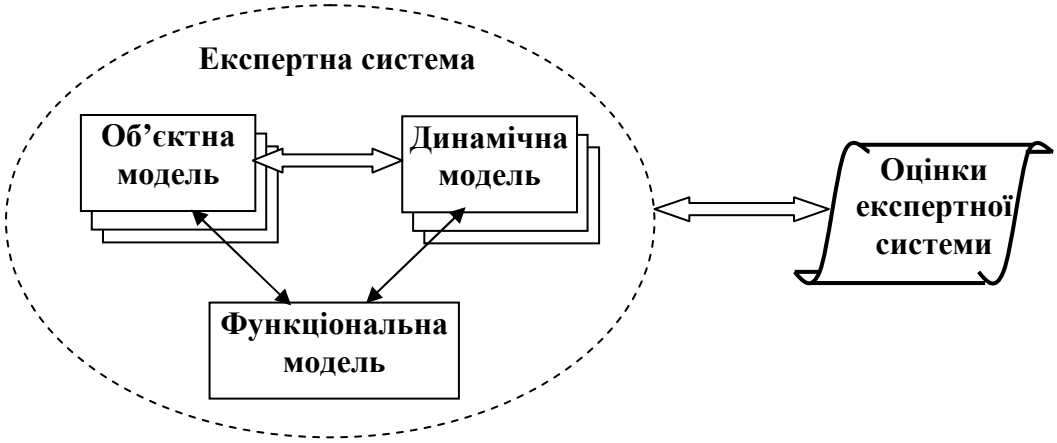

Рисунок 8.1 – Структура експертної системи

Для оцінки ступеня захищеності мереж *методами нечіткої логіки та нечітких множин вводяться лінгвістичні змінні*:

r – ступінь захищеності інформаційного ресурсу, яка забезпечується механізмом інформаційної безпеки у модулі безпеки компонента мережі;

s – ступінь ризику (ймовірність) здійснення загрози протягом певного проміжку часу;

p – величина можливих збитків, які можуть бути нанесені оператору внаслідок реалізації загроз.

Для оцінки ймовірності загрози вводяться декілька дискретних ступенів (градацій). Лінгвістичні змінні приймають терм-множину значень T_p, T_r і T_s відповідно

$$T_p = T_r = T_s = \{\text{“незначна”, “низька”, “середня”, “висока”}\}. \quad (8.2)$$

Межі 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 ступеня 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 з якою витрати на інформаційну безпеку $B_{\text{ІБ}}$ мають бути менші за можливі збитки $B_{\text{З}}$ за реалізації загроз: $B_{\text{ІБ}} < B_{\text{З}}$. Нечітку базу даних представляють у вигляді:

$$\bigcup_{l=1}^{k_j}[\bigcap_{i=1}^{n}\left(x_i = a_i^{jl}\right)] \to y = d_j;\ j = \overline{1,m};i = \overline{1,n}\,, \quad (8.3)$$

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 колективні застосовують нечітке відношення “між”, значення якого подається інтервалом значень на відрізку [0, 1]. Поняття “між” 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 за об'єкт *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 максимальний ступінь 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 удосконалення і розвитку системи оцінки інформаційної безпеки та отримання статистики технічної експлуатації КСЗІР.

8.2.2 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, отриманих методом експертного опитування.

Показники захищеності, гарантій, якості та взаємопов'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 параметрах 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 у 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 фактора, є основним.

Показники захищеності являють собою систему взаємопов'язаних і взаємозалежних компонентів; до номенклатури показників, крім 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 $B_{\text{ІБ}}$ мають бути менші за можливі збитки $B_{\text{З}}$ за реалізації загроз: $B_{\text{ІБ}} < B_{\text{З}}$.

Позначимо через X_1, …, 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 факторів. Наприклад, важко оцінити кількісно надійність зв'язку чи якість керування системою безпеки. При неможливості оцінки показника кількісно його оцінюють якісно, відображаючи міру прояви даної прикмети, застосовуючи порядкові шкали і користуючись методом експертного опитування.

Результатом оцінювання повинна бути матриця показників захищеності й 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, …, 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 й якості (табл. 8.1).

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:

$$B_{\text{ІБ1}} = \sum_{m=1}^{M} B_m(l_m) + \sum_{i=1}^{I} \sum_{m=1}^{M} B_{im}(l_{im}), \qquad (8.4)$$

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}.

Таблиця 8.1 – Матриця показників захищеності та якості телекомунікаційних мереж

Показники захищеності й якості	Оцінки показників для варіантів розподілу послуг забезпечення безпеки й 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	$B_{ІБ}$	$B_{ІБ}$	$B_{ІБ}$
Гарантій захисту	Рівень 1	Рівень 2	Рівень 3

У варіанті розподілу послуг безпеки між прикінцевими пунктами і вузлами мережі загальні витрати на інформаційну безпеку $B_{ІБ}$ можуть бути обчислені за виразом

$$B_{ІБ2} = N \sum_{m=1}^{M} B_m(l_m) + V \sum_{j=1}^{J} \sum_{m=1}^{M} B_{jm}(l_{jm}), \qquad (8.5)$$

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 (8.5) випливає, що загальні витрати можуть зменшитись, бо $V < N$. Залежність захищеності від перерозподілу засобів захисту у мережі пов’язана з конкретними параметрами послуг захисту.

8.2.3 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 (вирішуване 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.

За цим методом необхідна далі більш детальна оцінка відібраних варіантів.

Метод комплексного показника полягає в отриманні згортки показників до єдиного комплексного показника за формулами, одна з яких може мати вигляд:

$$F = \sum_{i=1}^{n} a_i X_i, \tag{8.6}$$

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 вирішуваних правил. Кожне правило базується на інформації, отримуваної від експерта. За допомогою вирішуваних правил проводиться часткове впорядкування (ранжирування) точок простору показників.

Задовільність деякого вирішуваного правила можна з'ясувати лише в процесі його застосування. Тому процедура вибору повинна бути трохи кроковою. Якщо вирішуване правило не забезпечує визначеності

впорядкування варіантів, то за наступним кроком має бути отримана додаткова інформація і побудоване більш “сильне” вирішуване правило, яке дозволило б усунути невизначеність впорядкування варіантів.

Інформацію, отримувану від експерта, необхідно перевіряти на змістовність, адекватність задачі і несуперечливість. Додаткова інформація на кожному кроці повинна порівнюватись з отриманою раніше. Тому процедура побудови вирішуваного правила повинна бути інтерактивною.

8.2.4 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 постанова задачі така. Задана область параметрів $P(x_1, \ldots, x_m)$ та цільові функції комплексного показника:

$$\begin{aligned} k_1 &= f(x_1, \ldots, x_m), \\ k_2 &= f(x_1, \ldots, x_m), \\ &\ldots \\ k_k &= X_n = f(x_1, \ldots, x_m), \end{aligned} \tag{8.7}$$

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. 8.2.

Спочатку формується загальна стратегія інформаційної безпеки, а на її базі – часткові стратегії варіантів побудови системи захисту. Формуються вимоги до системи захисту і початкове вирішуване правило.

В основному циклі процедури формуються варіанти побудови системи інформаційної безпеки на базі інформації експертів. Отримані варіанти ранжуються у просторі критеріїв і застосовується вирішуване 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” вирішуване правило. Перевагою цього методу є те, що збирається й 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 8.2 – Процедура вибору раціонального варіанта розподілу послуг

Далі розглянемо методику обґрунтування доцільності витрат на інформаційну безпеку ЦАТС, сутність поняття «оцінка витрат на захист інформації», модель та категорії витрат на захист інформаційних активів.

8.3 Економічне обґрунтування витрат на забезпечення систем інформаційної безпеки

8.3.1 Опис проблеми

Інтенсивний розвиток нових інформаційно-комунікаційних технологій (ІКТ) став не лише природною та необхідною умовою економічного та науково-технічного прогресу, а й породив цілий комплекс негативних наслідків, пов'язаних, перш за все, з появою реальної можливості використання цих технологій у протиправних цілях.

Забезпечення інформаційної безпеки є однією з найважливіших функцій держави [32] та одним із основних напрямів державної інформаційної політики [33].

Розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування визначається одним із пріоритетних напрямів державної політики. Однією з основних стратегічних цілей розвитку інформаційного суспільства в Україні є покращення стану інформаційної безпеки в умовах використання новітніх ІКТ. Національна політика розвитку інформаційного суспільства в Україні ґрунтується також і на засадах забезпечення інформаційної безпеки [34].

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю дій, які можуть призвести до витоку, розкрадання, втрати, спотворення, підробки, знищення, копіювання та блокування інформації.

У сучасних умовах особливо важливим є забезпечення безпеки об'єктів критичної інформаційної інфраструктури. Неправомірний доступ до інформації може порушити діяльність різних систем автоматизованого контролю та управління об’єктами життєзабезпечення, енергетики, оборони, транспорту, спричинити не лише значні матеріальні збитки, але й призвести до заподіяння шкоди здоров'ю людей та їх загибелі.

Саме тому власники, власники і користувачі інформаційних ресурсів повинні розуміти, що надійний захист інформації та гарантоване покриття ризиків можливі тільки за умови забезпечення належного рівня інформаційної безпеки (ІБ), яка є невід’ємною складовою кожної зі сфер національної безпеки і водночас важливою самостійною сферою забезпечення національної безпеки держави.

На сьогоднішній день у сфері ІБ однією з актуальних проблем є проблема забезпечення інформаційної безпеки в різних сферах економічної діяльності та оцінка витрат на захист інформації .

Загрози інформаційним активам не можуть бути виявлені, локалізовані та ліквідовані впровадженням в інформаційні системи та мережі окремих апаратних, програмних засобів та організаційних заходів. Частковий підхід до вирішення проблем ІБ неминуче призведе до неокупності вкладених інвестицій. Всі кошти і заходи повинні бути об'єднані у систему захисту інформації, що розглядається як регулярний процес, здійснюваний шляхом комплексного використання технічних, програмних засобів та організаційних заходів на всіх етапах життєвого циклу інформації [35].

Як показує досвід, однією з найбільш складних проблем забезпечення інформаційної безпеки є пояснення керівнику організації в дохідливій формі, чим саме займається колектив фахівців з інформаційної безпеки, чому на цю роботу потрібно витрачати значні фінансові та інші ресурси, чого саме можна очікувати в результаті цих витрат та як він особисто може переконатися в тому, що виділені ресурси не витрачені даремно [36].

При цьому далеко не завжди фахівці можуть обґрунтовано оцінити обсяг грошових інвестицій, необхідний для розв’язання задач інформаційної безпеки.

Станом на сьогоднішній день існують різні підходи щодо розуміння поняття та сутності економічного обґрунтування витрат на забезпечення систем захисту інформації, але будь-які готові рішення відсутні.

Українське законодавство не має визначення цього поняття, у зв'язку з чим практичному фахівцю, який реально займається питаннями забезпечення безпеки в організації, досить складно орієнтуватися, знайти відповіді на виникаючі питання і прийняти правильне рішення.

Враховуючи те, що Україна прагне стати повноправним членом глобального інформаційного суспільства, потреба у фахівцях з інформаційної безпеки буде збільшуватися. При цьому і вимоги до якості підготовки кваліфікованих фахівців з ІБ будуть зростати. Тому майбутні фахівці з ІБ повинні чітко зрозуміти, що без знань основ економіки ІБ неможливо забезпечити належний рівень захисту інформаційних активів організації відповідно до:

– вимог законодавства України в галузі ІБ;

– галузевих вимог щодо забезпечення ІБ;

– вимог нормативних, методичних та організаційно-розпорядчих документів щодо забезпечення ІБ;

– вимог національних та міжнародних стандартів у галузі ІБ.

Слід зазначити, що стандартів, які дозволяють оцінити ІБ з економічної точки зору, до цього часу відсутні. На момент написання даного посібника лише на стадії розробки знаходиться проект нового стандарту ISO/IEC WD TR 27016 «Information technology – Security

techniques – Information security management – Organizational economics», в якому пропонується, зокрема, зазначити: «Успішне управління ІБ вимагає суворого розуміння взаємозв'язку технічних (наприклад, баланс ризиків і безпеки) і економічних (наприклад, баланс переваг і витрат) підходів в усіх аспектах ІБ, починаючи від планування, дизайну і впровадження, та закінчуючи управлінням, поліпшенням та завершенням життєвого циклу. Концентрація тільки на технічних підходах застосування захисних заходів без урахування і розуміння впливу економічних факторів на «техніку» не забезпечить на належному рівні захист інформаційних активів організації [37]».

Звідси ми дійшли висновку, що витрати на ІБ необхідні для того, щоб за допомогою комплексу сучасних технічних, програмних та організаційних засобів забезпечити адекватний, тобто прийнятний для бізнесу рівень захищеності інформаційних активів організації. А говорити про ефективність вкладень в ІБ можна тільки після того, як організація сформулює вимоги до системи безпеки та створить єдину точку контролю та управління процесом забезпечення безпеки, призведе всю інфраструктуру та бізнес-процеси у відповідність з вимогами нормативних документів і стандартів.

8.3.2 Сутність поняття оцінка витрат на захист інформації

Необхідність у захисті інформації від стороннього втручання та спостереження давно усвідомлена, розроблені та продовжують розроблятися відповідні технології. Проте захоплення окремими рішеннями з області інформаційної безпеки прикриває фундаментальну проблему, а саме достатність та ефективність систем захисту з точки зору користувача. Мірилом споживчих якостей подібних систем може служити співвідношення «вартість/ефективність», тобто, в кінцевому рахунку, баланс між можливим збитком від несанкціонованих дій і розміром вкладень, які необхідно витратити для забезпечення захищеності інформаційних активів [38].

Хоча інформація, інформаційні системи та мережна інфраструктура давно стали суттєвими активами установ усіх форм власності, які мають матеріальну цінність, усе одно на практиці більшість рішень, спрямованих на захист інформації, приймаються на інтуїтивно-понятійному рівні, без будь-яких економічних розрахунків і обґрунтувань [39].

Сучасні вимоги бізнесу, що пред’являються до організації режиму інформаційної безпеки установ усіх форм власності, диктують нагальну необхідність використовувати в своїй роботі більш обґрунтовані техніко-економічні методи і засоби, що дозволяють кількісно вимірювати рівень захищеності організації, а також оцінювати економічну ефективність витрат на інформаційну безпеку.

Взагалі організація повинна визначити свої вимоги щодо інформаційної безпеки з урахуванням таких трьох факторів:

– по-перше, оцінка ризиків організації. За допомогою оцінки ризиків відбувається виявлення загроз активів організації, оцінка вразливості відповідних активів і ймовірності виникнення загроз, а також оцінка можливих наслідків;

– по-друге, визначити юридичні, законодавчі, регулюючі та договірні вимоги, яким повинні задовольняти організація, її торгові партнери, підрядники та постачальники послуг;

– по-третє, визначити специфічний набір принципів, цілей та вимог, розроблених організацією щодо оброблення інформації [40].

Оцінка ефективності організації інформаційної безпеки в організації передбачає оцінку витрат на захист інформації, а також оцінку досягнутого при цьому ефекту. Дійсно порівняння цих оцінок дозволяє оцінити повернення інвестицій на інформаційну безпеку, а також економічно коректно планувати й управляти бюджетом організації на інформаційну безпеку.

У загальному випадку підхід до оцінки ефективності організації інформаційної безпеки повинен включати три напрями:

- оцінка необхідності установки засобів захисту інформації в конкретній організації та ступеня раціональності прийнятих рішень;
- визначення конфігурації системи захисту інформації для заданого рівня ефективності;
- визначення необхідного обсягу фінансових витрат (інвестицій), потрібних для забезпечення прийнятих рішень [41].

Оцінка витрат на захист інформації – це розробка техніко-економічного обґрунтування вибору того чи іншого рішення для впровадження й експлуатації системи захисту інформації з точки зору економічних факторів. Крім того, розрахунок техніко-економічних показників дозволяє оцінити економічну ефективність впровадження або заміни системи захисту [42].

Згідно з ДСТУ 3396.1-96 можливі такі варіанти захисту інформації:

– досягнення необхідного рівня захисту інформації за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності;

– досягнення необхідного рівня захисту інформації за допустимих затрат і заданого рівня обмежень видів інформаційної діяльності;

– досягнення максимального рівня захисту інформації за необхідних затрат і мінімального рівня обмежень видів інформаційної діяльності [43].

Ідеальним рішенням є розв’язання задачі забезпечення інформаційної безпеки (по кожному *i*-му ризику) з мінімальними фінансовими витратами *Z* за максимальної ефективності *E* [44]:

$$\begin{cases} Z = \sum_i Zi \to \min, \\ E = \sum_i Ei \to \max. \end{cases} \qquad (8.8)$$

На жаль, подібне рішення навряд чи здійсненне і тому часто доводиться шукати компроміс між витратами на інформаційну безпеку та ймовірними загрозами. Яким має бути механізм пошуку цього компромісу?

У даний час не існує класифікації методик та моделей економічного обґрунтування вибору тих чи інших рішень з організації інформаційної безпеки. Основна причина полягає в тому, що існуючі підходи до захисту інформації засновані на нормативних документах, в основу яких покладено рекомендації або послідовності робіт з проведення аудиту інформаційної безпеки, розробки моделі загроз, визначення заходів щодо захисту від них і організації впровадження цих заходів. Економічна доцільність організаційних дій і технічних рішень до уваги не береться [44]. У разі появи вимоги щодо збереження державної таємниці подібний підхід цілком виправданий, особливо, коли мова йде про оборонні або військово-промислові підприємства, тому що найчастіше фінансування на інформаційну безпеку йде за рахунок бюджету, тобто для захисту інформації використовується третій варіант. У випадках, не пов'язаних з державною таємницею, оборонною промисловістю та іншими подібними ситуаціями, жорстке дотримання даними підходам не завжди має практичний сенс. У даному випадку захист інформації забезпечується, як правило, застосуванням першого або другого варіанта.

8.3.3 Модель витрат на захист інформаційних активів

Інвестиції в розроблення проекту системи захисту інформації, закупівлю необхідних елементів безпеки й експлуатацію систем захисту для власника інформації є не що інше, як матеріалізований економічний збиток. Йдучи на ці витрати, він сподівається уникнути більшого збитку, пов’язаного з можливим порушенням конфіденційності. Виникає дилема: внести плату (частково реалізувавши збиток) за можливість ухилення з часткою ймовірності або допустити можливість збитку повною мірою, не витрачаючи нічого. Розумне рішення полягає у визначенні оптимальних вкладень у системи захисту, що забезпечують мінімальні фінансові втрати власника інформації при несанкціонованих діях з нею. Отже, перед власником стоїть задача створення оптимальної, з економічної точки зору, системи захисту інформації.

Для того**,** щоб сформувати розуміння пріоритетності заходів щодо підвищення рівня безпеки, необхідно розробити механізм управління ризиками інформаційної безпеки, що дозволить спрямувати всі зусилля на захист від найбільш небезпечних загроз і мінімізацію витрат.

Під управлінням ризиками інформаційної безпеки розуміється взагалі процес виявлення, управління та зменшення ризиків інформаційної безпеки. Він включає в себе оцінку ризиків, аналіз витрат та вигод, а також вибір, впровадження, тестування й оцінку гарантій безпеки. Цей загальний огляд системи безпеки розглядається як ефективність і, в тому числі, вплив на місію та обмеження у зв'язку з політикою, правилами і законами [45].

Управління ризиками застосовується для захисту активів організації від ризиків, тобто подій випадкового і непередбачуваного характеру, які можуть завдати шкоди її діяльності. Для кожного з ризиків необхідно прийняти рішення щодо оброблення ризиків. Оброблення ризику – процес вибору та впровадження заходів щодо модифікації ризику. Можливі варіанти оброблення ризиків включають: а) застосування належного контролю для зниження ризиків; б) свідоме й об'єктивне прийняття ризиків із забезпеченням, що вони чітко задовольняють політику організації та критерії прийняття ризику; в) уникнення ризиків не дозволяючи дії, які можуть спричинити виникнення ризиків; г) перенесення пов'язаних ризиків на інші сторони, наприклад, страхувальників або постачальників [46].

Важливим моментом під час управління ризиками є обґрунтування та розподіл витрат на їх оброблення. Для кращого розуміння нижче продемонструємо графічну інтерпретацію витрат на інформаційну безпеку. Початкові положення та основні параметри можна визначити з наступних міркувань. Чим більший необхідний рівень захищеності інформаційних активів, тим потрібні більші витрати на побудову системи захисту. Для простоти залежність витрат на побудову системи безпеки від рівня захищеності (лінія 1 на рис. 8.3) будемо вважати лінійною майже на всьому інтервалі, крім ділянки з максимальним рівнем захищеності, оскільки для його досягнення необхідно будувати модель з повним перекриттям, що значно збільшує витрати. Залежність витрат**,** пов'язаних з відшкодуванням збитків (крива 2 на рис. 8.3), може бути апроксимована експоненційною кривою. Загальні збитки (крива 3 на рис. 8.3) виражаються сумою витрат на побудову системи захисту та витратами**,** пов'язаними з відшкодуванням збитків.

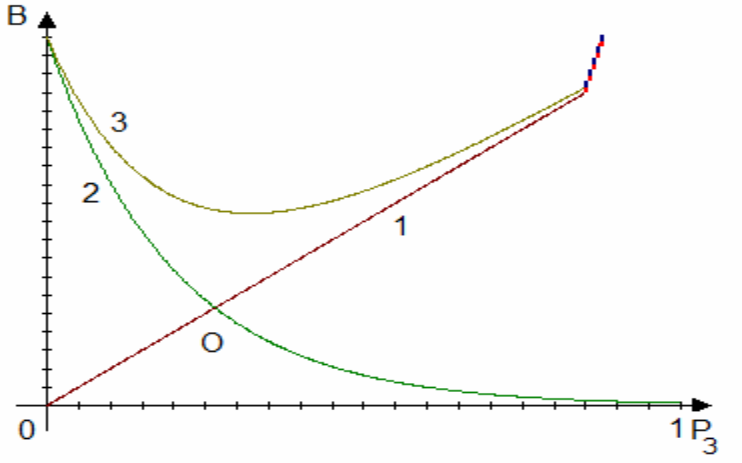

Рисунок 8.3 – Модель витрат на захист інформаційних активів

Точка О на рис. 8.3 – точка економічної рівноваги, яка відповідає випадку, коли величина можливих витрат на відшкодування збитків дорівнює витратам на впровадження системи безпеки. Вона є межею розумної достатності витрат на інформаційну безпеку [47].

Зазначимо, що заходи щодо оброблення ризиків поділяються на заходи**,** спрямовані на зниження ймовірності реалізації загрози та на заходи**,** спрямовані на зменшення наслідків**,** пов'язаних з реалізацією загрози. До перших, класичних, відносяться організаційно-технічні та програмно-апаратні заходи та засоби. До других – страхування, самострахування та інші.

Таким чином, вкладення коштів у систему захисту інформації вже в порівняно невеликих розмірах є дуже ефективним. За певної вартості системи захисту інформації ризик (загальні збитки) має найменше значення. Ця вартість є оптимальною.

В подальшому, понад оптимального значення, зростання витрат на системи захисту інформації буде вести до збільшення економічних втрат власника інформації.

Його виграш у підвищенні надійності системи захисту та відповідному зниженні ймовірності збитку від несанкціонованих дій буде знижуватися надзвичайно високою вартістю самої системи захисту.

Тому найкращою стратегією власника інформації буде, очевидно, використання системи захисту, що забезпечують мінімум ризику. Ефективність такого рішення підтверджується результатами чисельного моделювання, відповідно до яких використання економічно оптимальних систем захисту інформації призводить до зниження сумарних очікуваних втрат приблизно на порядок порівняно з базовими рішеннями.

8.3.4 Категорії витрат на інформаційну безпеку

Витрати на безпеку неможливо повністю виключити, проте вони можуть бути приведені до прийнятного рівня. Деякі види витрат на безпеку є абсолютно необхідними, а деякі можуть бути суттєво зменшені або виключені.

Останні – це ті, які можуть зникнути за відсутності порушень політики безпеки або скоротяться, якщо кількість і руйнівний вплив порушень зменшаться [48].

При дотриманні політики безпеки та проведенні профілактики порушень можна виключити або суттєво зменшити такі витрати:

• на відновлення інформаційних ресурсів установи;

• на реконструкцію системи інформаційного захисту інформації в установі;

• на юридичні суперечки і виплати компенсацій.

Необхідні витрати – це ті, які необхідні навіть якщо рівень загроз безпеки досить низький. Це витрати на підтримання досягнутого рівня захищеності інформаційного середовища підприємства.

Неминучі витрати можуть включати:

• обслуговування технічних засобів захисту інформації;

• конфіденційне та таємне діловодство;

• перевірки системи захисту інформації відповідності вимогам політики безпеки;

• навчання персоналу методам захисту інформації.

Взагалі витрати на інформаційну безпеку поділяються на такі категорії:

1. Витрати на формування та підтримку ланки управління системою захисту інформації (організаційні витрати).

1.1. Витрати на придбання і введення в експлуатацію програмно-технічних засобів: серверів, комп'ютерів кінцевих користувачів (настільні і мобільні), периферійних пристроїв і мережевих компонентів.

1.2. Витрати на придбання та налагодження засобів захисту інформації.

1.3. Витрати на утримання персоналу та аутсорсинг.

1.4. Витрати на формування політики безпеки підприємства.

2. Витрати на контроль (визначення та підтвердження досягнутого рівня захищеності ресурсів підприємства).

2.1. Планові перевірки та випробування:

– витрати на перевірки та 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 в підрозділах;

– оплата робіт з контролю правильності введення даних в прикладні системи;

– оплата інспекторів з контролю вимог, що пред'являються захисним засобам при розробці будь-яких систем (контроль виконується на стадії проектування та специфікації вимог).

2.2. Позапланові перевірки і випробування:

– оплата роботи випробувального персоналу спеціалізованих організацій;

– забезпечення випробувального персоналу (внутрішнього і зовнішнього) матеріально-технічними засобами.

2.3. Контроль за дотриманням політики інформаційної безпеки:

– витрати на контроль реалізації функцій, що забезпечують управління захистом комерційної таємниці;

– витрати на організацію тимчасової взаємодії і координації між підрозділами для вирішення конкретних повсякденних 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.

2.4. Витрати на зовнішній аудит:

– витрати на контрольно-перевірочні заходи, пов'язані з ліцензійно-дозвільною діяльністю у сфері захисту інформації.

3. Внутрішні витрати на ліквідацію наслідків порушень політики інформаційної безпеки (витрати, понесені організацією в результаті того, що необхідний рівень захищеності не було досягнуто).

3.1. Перегляд політики інформаційної безпеки підприємства (проводиться періодично):

– витрати на ідентифікацію загроз безпеки;

– витрати на пошук вразливостей системи захисту інформації;

– оплата роботи фахівців, які виконують роботи з визначення можливого збитку і переоцінку ступеня ризику.

3.2. Витрати на ліквідацію наслідків порушення режиму інформаційної безпеки:

– відновлення системи безпеки до відповідності вимогам політики безпеки;

– установка патчів або придбання останніх версій програмних засобів захисту інформації;

– придбання технічних засобів замість тих, що прийшли в непридатність;

– проведення додаткових випробувань і перевірок технологічних інформаційних систем;

– витрати на утилізацію скомпрометованих ресурсів.

3.3. Відновлення інформаційних ресурсів підприємства:

– витрати на відновлення баз даних та інших інформаційних масивів;

– витрати на проведення заходів з контролю достовірності даних, що піддалися атаці на цілісність.

3.4. Витрати на виявлення причин порушення політики безпеки:

– витрати на проведення розслідувань порушень політики безпеки (збір даних про способи вчинення, механізм і способи приховування неправомірного діяння, пошук слідів, знарядь, предметів посягання, виявлення мотивів неправомірних дій тощо);

– витрати на оновлення планів забезпечення безперервності діяльності служби безпеки.

3.5. Витрати на переробки:

– витрати на впровадження додаткових засобів захисту, які потребують суттєвої перебудови системи безпеки;

– витрати на повторні перевірки та випробування системи захисту інформації.

4. Зовнішні витрати на ліквідацію наслідків порушення політики інформаційної безпеки.

4.1. Зовнішні витрати на ліквідацію наслідків порушення політики безпеки:

– зобов'язання перед державою та партнерами;

– витрати на юридичні суперечки і виплати компенсацій;

– втрати в результаті розриву ділових стосунків з партнерами.

4.2. Втрата новаторства:

– витрати на проведення додаткових досліджень та розробки нової ринкової стратегії;

– відмова від організаційних, науково-технічних або комерційних рішень, які стали неефективними в результаті витоку відомостей 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.

4.3. Інші витрати:

– заробітна плата секретарів і службовців, організаційні та інші витрати, які безпосередньо пов'язані з попереджувальними заходами;

– інші види можливих збитків підприємству, в тому числі пов'язані з неможливістю виконання функціональних завдань, визначених його Статутом.

5. Витрати на технічне обслуговування системи захисту інформації та заходи щодо запобігання порушень політики безпеки підприємства (попереджувальні заходи).

5.1. Витрати на управління системою захисту інформації:

– витрати на планування системи захисту інформації підприємства;

– витрати на вивчення можливостей інформаційної інфраструктури підприємства щодо забезпечення безпеки інформації обмеженого поширення;

– витрати на здійснення технічної підтримки виробничого персоналу при впровадженні засобів захисту та процедур, а також планів щодо захисту інформації;

– перевірка співробітників на лояльність, виявлення загроз безпеки;

– організація системи допуску виконавців і співробітників конфіденційного діловодства з відповідними штатами та оргтехнікою.

5.2. Регламентне обслуговування засобів захисту інформації:

– витрати, пов'язані з обслуговуванням і налаштуванням програмно-технічних засобів захисту, операційних систем і використовуваного мережного обладнання;

– витрати, пов'язані з організацією мережевої взаємодії і безпечного використання інформаційних систем;

– витрати на підтримку системи резервного копіювання та ведення архіву даних;

– проведення інженерно-технічних робіт з встановлення сигналізації, обладнання сховищ конфіденційних документів, захисту телефонних ліній зв'язку, обчислювальної техніки тощо.

5.3. Аудит системи безпеки:

– витрати на контроль змін стану інформаційного середовища підприємства;

– витрати на систему контролю за діями виконавців.

5.4. Забезпечення належної якості інформаційних технологій:

– витрати на забезпечення відповідності вимогам якості інформаційних технологій, у тому числі аналіз можливих негативних аспектів інформаційних технологій, які впливають на цілісність та доступність інформації;

– витрати на доставку (обмін) конфіденційної інформації;

– задоволення суб'єктивних вимог користувачів: стиль, зручність інтерфейсу тощо.

5.5. Забезпечення вимог стандартів:

– витрати на забезпечення відповідності прийнятим стандартам і вимогам, достовірності інформації, дієвості засобів захисту.

5.6. Навчання персоналу:

– підвищення кваліфікації співробітників підприємства в питаннях використання наявних засобів захисту, виявлення і запобігання загроз безпеки;

– розвиток нормативної бази служби безпеки [49].

8.4 Методи оцінки економічної ефективності систем захисту інформації

Для оцінки економічної ефективності систем захисту інформації, планування інформаційної безпеки та управління нею на основі концепції управління ризиками можна скористатися наступними методами:

– прикладного інформаційного аналізу (Applied Information Economics, AIE);

– розрахунку споживчого індексу (Customer Index, CI);

– розрахунку доданої економічної вартості (Economic Value Added, EVA);

– визначення початкової економічної вартості (Economic Value Sourced, EVS);

– управління портфелем активів (Portfolio Management, PM);

– оцінки дійсних можливостей (Real Option Valuation, ROV);

– підтримки життєвого циклу штучних систем (System Life Cycle Analysis, SLCA);

– розрахунку системи збалансованих показників (Balanced Scorecard, BSC);

– розрахунку сукупної вартості володіння (Total Cost of Ownership, TCO);

– функціонально-вартісного аналізу (Activity Based Costing, ABC) [19].

Зокрема, для розрахунку видаткової частини на технічну архітектуру забезпечення інформаційної безпеки рекомендується використовувати метод сукупної вартості володіння (TCO), а для обґрунтування інвестицій в корпоративну систему захисту інформації – метод очікуваних втрат, оцінки властивостей системи безпеки, а також аналізу «дерева» помилок.

Метод сукупної вартості володіння (***Total Cost of Ownership***, ***TCO***). Даний метод був запропонований компанією Gartner Group в кінці 80-х

років (1986-1987). ТСО є ключовим показником інформаційних технологій та інформаційних систем в організації, тому що дозволяє оцінювати сукупні витрати на інформаційні технології, аналізувати їх і, відповідно, управляти ІТ-витратами для досягнення найкращої віддачі.

Основною метою методу розрахунку сукупної вартості володіння є виявлення надлишкових статей витрат та оцінка можливості повернення інвестицій, вкладених в технології безпеки.

При цьому, отримані дані щодо сукупної вартості володіння використовуються для виявлення видаткової частини використання системи захисту інформації установи.

У цілому визначення витрат установи на інформаційну безпеку має на увазі рішення наступних трьох завдань:

– оцінку поточного рівня ТСО системи захисту інформації установи;

– аудит інформаційної безпеки установи на основі порівняння рівня захищеності установи та рекомендованого (краща світова практика) рівня ТСО;

– формування цільової моделі ТСО.

Оцінка поточного рівня ТСО

У ході робіт з оцінки ТСО відбувається збирання інформації та розрахунок показників ТСО організації за такими напрямами:

– існуючі компоненти інформаційної системи (включаючи систему захисту інформації) та інформаційні активи установи (сервери, комп'ютери клієнтів, периферійні пристрої, мережні пристрої);

– існуючі витрати на апаратні і програмні засоби захисту інформації (матеріали, амортизація);

– існуючі витрати на організацію інформаційної безпеки в установі (обслуговування системи захисту інформації, а також штатних засобів захисту периферійних пристроїв, серверів, мережних пристроїв, планування й управління процесами захисту інформації, розробку концепції та політики безпеки тощо);

– існуючі витрати на організаційні заходи захисту інформації;

– існуючі непрямі витрати на організацію інформаційної безпеки установи і, зокрема, забезпечення безперервності або стійкості бізнесу.

Аудит інформаційної безпеки установи

За результатами співбесіди з керівництвом організації і проведення інструментальних перевірок рівня захищеності організації проводиться аналіз наступних основних аспектів:

– політики безпеки;

– організації захисту;

– класифікації та управління інформаційними активами;

– управління персоналом:

– фізичної безпеки;

– адміністрування комп'ютерних систем і мереж;

– управління доступом до систем;

– розробки та супроводу систем;

– планування безперебійної роботи організації;

– перевірки системи на відповідність вимогам інформаційної безпеки.

На основі проведеного аналізу вибирається модель ТСО, порівняна з середніми та оптимальними значеннями для групи аналогічних організацій, що мають схожі з розглянутою організацією показники за обсягом бізнесу. Така група вибирається з банку даних по ефективності витрат на інформаційну безпеку та ефективності відповідних профілів захисту аналогічних компаній.

Порівняння поточного показника ТСО перевіряється з модельним значенням показника ТСО дозволяє провести аналіз ефективності організації ІБ організації, результатом якого є визначення «вузьких» місць в організації, причин їх появи і вироблення подальших кроків щодо реорганізації системи захисту інформації та забезпечення необхідного рівня захищеності установи.

Формування цільової моделі ТСО

За результатами проведеного аудиту моделюється цільова (бажана) модель, що враховує перспективи розвитку бізнесу та корпоративної системи захисту інформації (активи, складність, методи кращої практики, типи систем захисту інформації, кваліфікація співробітників компанії тощо).

Крім того, розглядаються капітальні витрати і трудовитрати, необхідні для проведення перетворень поточного середовища в цільове середовище. До трудовитрат на впровадження включаються витрати на планування, розгортання, навчання і розроблення. Сюди ж входять можливі тимчасові збільшення витрат на управління і підтримку.

Основні положення та приклад використання методики можна знайти в [49].

Метод очікуваних втрат (***Annualized Loss Expectancy, ALE***). Цей підхід базується на обчисленні втрат від порушень політики безпеки, з якими може зіткнутися організація, і їх порівнянні з інвестиціями в безпеку, спрямованими на запобігання порушень. Метод очікуваних втрат заснований на емпіричному досвіді організацій та відомостей про вторгнення, про втрати від вірусів, про відображення сервісних нападів тощо. Наприклад, порушення безпеки призводять організації до наступних фінансових втрат, пов’язаних з:

- зниженням рівня довіри з боку клієнтів та інвесторів;
- зайвими експлуатаційними витратами;
- одноразовими витратами, що виникають внаслідок безпосередньої втрати активу або його частини;
- втратою робочого часу і, як наслідок – зниження конкурентоспроможності;
- штрафами, судовими переслідуваннями та перевірками з боку контролюючих органів.

Для того щоб зменшити ймовірні втрати, організації необхідно інвестувати кошти в інформаційну безпеку: антивіруси, мережні екрани, системи виявлення вторгнень, DLP-системи тощо. Якщо установа вирішує впровадити систему захисту інформації, то її вартість узагальнено буде складатися з одноразових і періодичних витрат.

Фінансова вигода забезпечується щорічними заощадженнями, які отримує компанія при впровадженні системи інформаційної безпеки. Вигода розраховуються за такою формулою:

$$AS = ALE \times E - AC, \tag{8.9}$$

де *AS* – щорічні заощадження (*Annual Saving*); *ALE* – показник очікуваних втрат (*Annualised Loss Expectancy*); *E* – ефективність системи захисту (близько 85%); *AC* – щорічні витрати на безпеку (*Annual Cost*).

Оцінка очікуваного можливого збитку від одиничної реалізації певної загрози (*Single Loss Exposure, SLE*) розраховується за формулою:

$$SLE = AV \times EF. \tag{8.10}$$

Підсумкові очікувані втрати від конкретної загрози за певний період часу (*Annual Loss Exposure, ALE*) характеризують величину ризику і розраховуються за формулою:

$$ALE = SLE \times ARO. \tag{8.11}$$

Приклад використання даного методу розкрито в посібнику «Менеджмент інформаційної безпеки в галузі зв'язку» [51].

Метод оцінки властивостей системи безпеки (***Security Attribute Evaluation Method, SAEM***) був розроблений в Carnegie Melon University та заснований на порівнянні різних архітектур систем інформаційної безпеки для фінансової оцінки вигод від їх впровадження. Методологія SAEM полягає в тому, щоб, оцінивши існуючі ризики, запропонувати різні проекти з інформаційної безпеки, що різняться за вартістю та ефективністю. Недолік методу полягає в тому, що найчастіше безпека перебуває поза розумінням менеджерів, які займаються оцінкою ефективності, а фахівці з інформаційної безпеки рідко мають точні дані щодо вигод, принесених технологією, тому доводиться покладатися на досвід та інтуїцію і на їх основі приймати рішення. Проте цей метод може бути використаний для подання комплексу різноманітних заходів з інформаційної безпеки та для підтримки прийняття рішення при виборі тих чи інших заходів.

Нетрадиційним інструментом оцінки вигод є метод аналізу «дерева помилок» (***Fault Tree Analysis***). Мета застосування даного методу – показати, в чому полягають причини порушень політики безпеки, і які контрзаходи можуть бути застосовані.

Контрзаходи щодо забезпечення безпеки спрямовані на досягнення наступних ефектів: зменшення ймовірності походження інциденту та/або

зменшення наслідків, якщо інцидент усе одно трапляється. Заходи, що знижують вірогідність, називаються *профілактичними*, а заходи, що знижують наслідки, називаються *лікувальними*, наприклад, наявність резервних режимів роботи. До профілактичних заходів відносять, зокрема, аудит системи безпеки, установку мережних екранів, систем виявлення вторгнень, антивірусів, засобів шифрування, а також впровадження стандартів, процедур, посадових інструкцій та формування архівів. Планування безперервності бізнесу, а також відновлення бізнесу, навчання персоналу є як профілактичними заходами, так і лікувальними.

«Дерево помилок» – це графічний засіб, який дозволяє звести всю систему можливих порушень до логічних відносин *І-АБО* компонентів цієї системи. Якщо доступні дані за нормами відмови критичних компонентів системи, то «дерево помилок» дозволяє визначити очікувану ймовірність відмови всієї системи.

Застосовуючи цей метод до систем інформаційної безпеки, можна побудувати «дерево» з причинно-наслідковими відносинами між атаками на систему та порушеннями системи. Використання контрзаходів щодо запобігання порушень дозволяє нейтралізувати атаки.

При цьому може бути визначений ефект від впровадження контрзаходів безпеки на підставі порівняння структури «двох дерев» з використанням контрзаходів і без [52].

Метод компанії IBM. Фахівцями компанії IBM була запропонована емпірична залежність очікуваних втрат від i -ї загрози безпеки [53]:

$$R_i = 10^{(S_i + V_i - 4)}, \tag{8.12}$$

де S_i – коефіцієнт, що характеризує можливу частоту виникнення i-ї загрози; V_i – коефіцієнт, що характеризує значення можливого збитку при її виникненні.

Значення коефіцієнтів, які слід використовувати, представлені в табл. 8.2, 8.3.

Таблиця 8.2 – Рекомендовані значення S_i

Очікувана частота появи загрози	Рекомендоване значення S_i
Майже ніколи	0
1 раз на 1000 років	1
1 раз на 100 років	2
1 раз на 10 років	3
1 раз на рік	4
1 раз на місяць (приблизно 10 раз на рік)	5
2 рази на тиждень (100 раз на рік)	6
3 рази на день (1000 раз на рік)	7

Таблиця 8.3 – Рекомендовані значення V_i

Значення ймовірних збитків при реалізації загрози, грн.	Рекомендоване значення V_i
1	0
10	1
100	2
1000	3
10000	4

При цьому сумарна вартість втрат визначається за формулою:

$$R = \sum_i R_i \,. \tag{8.13}$$

Перевагою даного методу є його простота, недоліком – необхідність використання статистики, що відображає частоту виникнення тих чи інших загроз.

Висновки. Враховуючи сучасні вимоги до бізнесу, одним із основних видів витрат організації є витрати на інформаційну безпеку, необхідні для забезпечення адекватного, тобто прийнятного рівня захищеності інформаційних активів. Складне фінансове положення, в якому знаходяться українські організації, диктує нагальну необхідність використовувати в своїй роботі більш обґрунтовані техніко-економічні методи і засоби, що дозволяють кількісно вимірювати рівень захищеності організації, а також оцінювати економічну ефективність витрат на інформаційну безпеку.

На сьогоднішній день витрат на інформаційну безпеку неможливо повністю уникнути, проте вони можуть бути приведені до прийнятного рівня. Для того**,** щоб сформувати розуміння пріоритетності заходів щодо підвищення рівня безпеки, необхідно розробити механізм управління ризиками інформаційної безпеки, що дозволить спрямувати всі зусилля на захист від найбільш небезпечних загроз і мінімізацію витрат. Для оцінки економічної ефективності систем захисту інформації, планування інформаційної безпеки та управління нею на основі концепції управління ризиками у розділі наведено низку методів, а саме: метод оцінки сукупної вартості володіння, метод оцінки властивостей системи безпеки, метод очікуваних втрат, метод аналізу «дерева помилок» та метод компанії IBM.

Отже, підсумовуючи все вищезазначене можна сказати, що сучасний фахівець з інформаційної безпеки повинен чітко вирішувати завдання створення оптимальної, з економічної точки зору, системи захисту інформації.

Питання 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:

1) диференційний метод;
2) метод багатокритеріального оцінювання;
3) метод комплексного показника;
4) інтерактивний метод.

9. Поясніть алгоритм вибору оптимального варіанта побудови системи інформаційної безпеки методом розв’язання задачі багатокритеріального вибору.

10. Які фактори спричиняють необхідність побудови економічно обґрунтованих систем захисту інформації?

11. Які проблеми виникають під час побудови економічно обґрунтованих систем захисту інформації?

12. На підставі яких факторів організації визначають вимоги до системи інформаційної безпеки?

13. Які варіанти побудови системи захисту інформації виділяють згідно з ДСТУ 3396.1-96?

14. Розкрийте можливі варіанти оброблення ризиків.

15. Опишіть модель витрат на захист інформаційних активів

16. Які категорії витрат на інформаційну безпеку можна визначити?

17. Розкрийте сутність методу сукупної вартості володіння.

18. Розкрийте сутність методу очікуваних втрат.

19. Розкрийте сутність методу оцінки властивостей системи безпеки.

20. Розкрийте сутність методу аналізу «дерева помилок».

21. Розкрийте сутність методу компанії IBM.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AMP – (Administration and maintenance plat)
Плата адміністрування та технічного обслуговування

BAM – (Back Administration Module)
Системний модуль адміністрування

BS – (Base station) Базова станція

BSS – (Base Station Subsystem) Підсистема базових станцій

CCTV – (Closed-circuit television)
Система телебачення замкнутого контура

CDMA – (Code Division Multiple Access)
Множинний доступ з кодовим розподіленням

CPM – (Central Processing Module) Центральний модуль оброблення

GPRS – (General Packet Radio Service)
Стандарт, який використовує не зайняту голосовим зв'язком смугу частот для передавання інформації. Використовується в мобільних пристроях для передавання MMS, WAP-серфінгу та повноцінного з'єднання з мережею Інтернет

GSM – (Global System for Mobile Communications)
Глобальний стандарт цифрового мобільного стільникового зв’язку

GSPC – Плата полки пристроїв мережної комутації, забезпечує оброблення даних і підтримку глобальних послуг

GVDP – Плата в модулі CPM, що реалізує функцію управління базою даних з інформацією про користувачів

IGWB (i-Gateway Bill) Інтегрований шлюз білінгового центру

ITU – (International Telecommunication Union)
Міжнародний Союз Електрозв’язку

MMU – (Management module unit) Модуль керування ЗП

MSC – (Mobile Switching Centers) Центр мобільної комутації

NGN – (Next Generation Networks) Мережі третього покоління

SPM – (Services processing module) Модуль оброблення послуг

SSD – (Shared Secret Data)
Спільно використовувані дані засекречування

TCO – (Total Cost of Ownership) Загальна вартість володіння

TUP – (Telephone User Part)
Підсистема користувача телефонної мережі

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 оброблення викликів служби «Міліція»
ОІД – Об'єкт інформаційної діяльності
ПЕМВН – Побічні електромагнітні випромінювання та наводок
ПЦС УДПО – Пульт центрального спостереження управління державної пожежної охорони
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 оброблення викликів
ЦСК – Цифрові системи комутації

ПЕРЕЛІК ПОСИЛАНЬ

1. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посіб./Кормич Б.А. – 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 /В.Я Рубан // 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 зі 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./ Черноруцкий И.Г. –СПб., 2001. – С. 248.

22. Организация планирование и управление предприятиями связи / [Демина Е.В., Иодко Е.К., Майофис Л.И., Резникова Н.П.]. – М.: Радио и связь, 1990. – 352 с.

23. Котенко М. Центры обработки вызовов / М. Котенко // Телеком. – 2000. – № 9-10 (27-28). – С. 56-63.

24. Гольдштейн Б.С. Центры обработки вызовов для органов внутренних дел: учеб. пособ. / Гольдштейн Б.С., Зарубин А.А., Потапов А.И. // 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 / Шварц М.; пер. с англ. под ред. В. А.Жожикашвили. – М.: Радио и связь, 1981. – 336 с.

27. Корнышев Ю.Н. Задачник по теории телефонных и телеграфных сообщений. / Корнышев Ю.Н., Мамонтова Н.П. – Одесса: ОЭИС, 1974. – 139 с.

28. Корявцев П.М. Общий комплекс мер по обеспечению инфрмационной безопасности: метод. рекоменд. / Корявцев П.М. // 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 / Бельфер Р. А. // Электросвязь – 2002. – № 7. – С. 14-18.

32. Конституція України (станом на 12.04.12 р.) – Верховна Рада України [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

33. Закон України «Про інформацію» від 02.10.1992 № 2657–XII [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657–12.

34. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 № 537-V [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/537-16.

35. Войтов И.В. Защита информации – важная составляющая научно-технического обеспечения информатизации и информационно-коммуникационной поддержки инновационного развития страны [Електронний ресурс]. – Режим доступу: http://aercom.by/wp-content/uploads/2011/07/sbornik-1.pdf.

36. Андрианов В.В Обеспечение информационной безопасности бизнеса [Електронний ресурс]. – Режим доступу: http://lib.rus.ec/b/370871/read.

37. Проект ISO 27016 [Електронний ресурс]. – Режим доступу: http://lukatsky.blogspot.com/2011/12/iso-27016.html.

38. Отчет о экономических параметрах создания инфраструктуры (включая каналы связи) системы [Електронний ресурс]. – Режим доступу: http://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFkQFjAA&url=http%3A%2F%2Faisup.economy.gov.ru%2Fpubportal%2Fdownloadfile%3Fuuid%3Dpprtflo2k03380000h6ja5dpqf3o16no&ei=5a7MT8jaGeSn4gSIlo2rCg&usg=AFQjCNGTjCwN5UWrh9hfZVP_oToImfg2GA&sig2=cTJD0ltrLVXjw9xYTin7FQ.

39. Сергей Петренко. Оценка затрат компании на информационную безопасность [Електронний ресурс]. – Режим доступу: http://www.bre.ru/security/18881.html.

40. Что такое информационная безопасность? [Електронний ресурс] – Режим доступу: http://prikladnayainformatika.ru/ib/156.

41. Вепрев С.Б. Новый подход к рациональному выбору технических средств обеспечения информационной безопасности объекта [Електронний ресурс]. – Режим доступу: http://www.st-s.su/publications/2008/1/articles/veprev/index.htm.

42. Оценка затрат на защиту информации [Електронний ресурс]. – Режим доступу: http://www.nwaktiv.ru/security/ocenkazatr.php.

43. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт».

44. Минзов А.С. Обоснование управленческих решений в сфере обеспечения информационной безопасности / А.С.Минзов, С.М.Кольер // Электронный журнал «Системный анализ в науке и образовании». – Вып. №1, 2010.

45. NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

46. Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою: СОУ Н НБУ 65.1 СУІБ 2.0:2010 . – К.: Національний банк України, 2010. – 209 с.

47. Копитін Ю.В. Модель страхування ризиків інформаційної безпеки./ Копитін Ю.В. // Цифрові технології. – 2010№ 8. [Електронний ресурс]. – Режим доступу: http://digitech.onat.edu.ua/files/13.pdf.

48. Сергей Петренко. Информационная безопасность: экономические аспекты /Сергей Петренко, Сергей Симонов, Роман Кислов [Електронний ресурс]. – Режим доступу: http://citforum.ru/security/articles/sec/index.shtml.

49. Петренко С.А. Оценка затрат на кибербезопасность // Труды ИСА РАН, 2006. – Т.27 [Електронний ресурс]. – Режим доступу: http://www.isa.ru/proceedings/images/documents/2006-27/234-265.pdf.

50. Сидоров А.О. Модель и метод структурированной оценки риска при анализе информационной безопасности [Електронний ресурс]. – Режим доступу: http://aspirantura.ifmo.ru/file/other/aO5gQaS2GS.pdf.

51. Тардаскіна Т.М. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посіб./ Т.М. Тардаскіна, В.Г. Кононович – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 268 с.

52. Сергей Петренко. Обоснование инвестиций в безопасность / Сергей Петренко, Елена Терехова [Електронний ресурс]. – Режим доступу: http://www.osp.ru/cio/2006/01/379802/.

53. Кутузов Д.В. Методы оценки рисков, связанных с нарушением информационной безопасности предприятия / Д. В. Кутузов, В.Н. Белозеров, Р. О. Ларченко [Електронний ресурс]. – Режим доступу: http://www.aspu.ru/images/File/Izdatelstvo/pricaspiiskii/3.pdf.

54. M800 CDMA Mobile Switching Centre System Description – working documents

55. Гарсия М. Проектирование и оценка систем физической защиты / Гарсия М.; пер. с англ. под ред. Р.Г. Магауенова. – М.: Мир, 2003.

56. Техническая безопасность объектов предпринимательства. – I том /Сост. Дворский М. Н., Палатченко С. Н. – К.: "А-ДЕПТ", 2006. – 304 с. ("Концепции безопасности").

Література для самостійного ознайомлення:

54. Ларина И.Е. Экономика защиты информации: учеб. пособ. / Ларина И.Е. – М.: МГИУ, 2007. – 92 с.

55. Цуканова О.А. Экономика защиты информации: учеб. пособ. / Цуканова О.А., Смирнов С.Б. – СПб.: СПб ГУИТМО, 2007. – 59 с.

ЗМІСТ

Навчальне видання

Кононович Володимир Григорович,
Стайкуца Сергій Володимирович,
Лемеха Тетяна Миколаївна,
Копитін Юрій Вікторович

ІНФОРМАЦІЙНА БЕЗПЕКА ЦИФРОВИХ ПРОГРАМНО-КЕРОВАНИХ АТС

Навчальний посібник для курсового та дипломного проектування

Редактор *Л.А. Кодрул*
Комп'ютерне верстання *Ж.А. Гардиман*

Видавець і виготовлювач ОНАЗ ім. О.С. Попова
(Свідоцтво ДК № 3633 від 27.11.09)
м. Одеса, вул. Ковальська, 1

Здано до набору 14.12.11. Підписано до друку 11.05.12.
Обсяг 11,7 ум.-друк. арк.
Формат 90×60/16. Зам. № 4853. Наклад 300 прим.
Віддруковано на видавничому устаткуванні фірми RISO
в друкарні редакційно-видавничого центру ОНАЗ ім. О.С. Попова
Одеса, 65021, вул. Ковалевського, 5
Тел. (0482) 70-50-494