**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА** **КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Засоби підвищення рівня захищеності інформаційно-комунікаційних систем від витоку конфіденційних даних

|  |  |
| --- | --- |
| **Автор:** | А.О. Манжула |
| **Науковий керівник:** д.т.н., проф. | М.Б. Гумен |
| **Нормоконтролер:** асист. | С.В. Єгоров |

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:**Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Комп’ютеризованих систем захистуінформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма:** «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_С.В. Казмірчук

«\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Манжули Андрія Олександровича**

1. Тема роботи «Засоби підвищення рівня захищеності інформаційно комунікаційних систем від витоку конфіденційних даних»

затверджена наказом ректора від 02.10.2019 р. № 2265/ст.

1. Термін виконання роботи: з 14.10.2019 р. по \_\_\_\_.06.2018 р.
2. Вихідні дані роботи: проаналізувати існуючі системи та методики аналізу і оцінки ризиків інформаційної безпеки; на основі аналізу виділити вхідні і вихідні параметри, виявлення їх переваг і недоліків систем; розробити методику, алгоритм та програмне забезпечення підвищення захисту системи.
3. Зміст пояснювальної записки:. аналіз існуючих систем та методик аналізу і оцінки ризиків інформаційної безпеки; розробка програмного модуля DLP-cистем, верифікація отриманих результатів.
4. Перелік обов'язкового ілюстративного матеріалу: таблиці, рисунки, презентація.
5. Календарний план-графік

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
|  | Огляд джерел за темою та напрям досліджень | 18.09.2019-06.10.19 | *Виконано* |
|  | Методи досліджень | 07.10.19-24.11.19 |  |
|  | Результати досліджень | 25.11.19-15.12.19 |  |
|  | Виконання технічного розділу | 16.12.19-29.12.19 |  |
|  | Оформлення і друк пояснювальної записки | 30.12.19-10.01.20 |  |

Керівник дипломної роботи: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (П.І.Б)

**УДК**

**РЕФЕРАТ**

Пояснювальна записка до дипломної роботи «Засоби підвищення рівня захищеності інформаційно комунікаційних систем від витоку конфіденційних даних»: 101 с., 7 рис., 8 табл., 26 літературне джерело.

Об’єкт дослідження: система запобігання витоку інформації.

Предмет дослідження: Засоби захисту ІКС

Мета дипломної роботи: підвищення рівня захищеності інформаційнотелекомунікаційних систем.

Методи дослідження: засоби підвищення рівня захищеності ІКС

Отримані результати: захищені канали передачі інформації.

Наукова новизна роботи полягає у удосконаленні захисту ІКС на базі АТС за домогою програмного модулю.

Розглянуті моделі управління інформаційною безпекою призначена для функціонування на підприємствах з метою попередження витоків ІзОД.

**ЗМІСТ**

[**УМОВНІ ПОЗНАЧЕННЯ** 7](#_Toc31009361)

[**ВСТУП** 9](#_Toc31009362)

[**РОЗДІЛ I** 11](#_Toc31009363)

[**ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНО КОМУНІКАЦІЙНИХ СИСТЕМ** 11](#_Toc31009364)

[1.1. Поняття інформаційної комунікаційної системи 11](#_Toc31009365)

[**1.2 Основною метою системи захисту інформації є:** 12](#_Toc31009366)

[**1.3 Принципи організації безпеки мережевої інфраструктури** 14](#_Toc31009367)

[**1.5 Джерело загроз** 19](#_Toc31009368)

[**1.6 Виток інформації** 24](#_Toc31009369)

[**1.7 Основні принципи реалізації програмно-технічних засобів захисту інформації** 26](#_Toc31009370)

[**1.8 Політика інформаційної безпеки в ІКС** 28](#_Toc31009371)

[**1.9 Криптографічні засоби захисту інформації** 28](#_Toc31009372)

[**1.10 Методи та засоби захисту** 33](#_Toc31009373)

[**1.11 Організаційні заходи** 33](#_Toc31009374)

[**1.12 Інженерно-технічні заходи** 34](#_Toc31009375)

[**1.13 Рекомендації із захисту інформації, яка обробляється** 35](#_Toc31009376)

[**1.14 Висновки** 38](#_Toc31009377)

[**РОЗДІЛ II** 39](#_Toc31009378)

[**ЗАХИСТ АВТОМАТИЗОВАНИХ ТЕЛЕФОНИХ СТАНЦІЙ** 39](#_Toc31009379)

[**2.1 Модель цифрового вузла комутації з позицій технічного захисту інформації** 39](#_Toc31009380)

[**2.2 Загрози для інформації та моделі порушників** 44](#_Toc31009381)

[**2.3 Загальні положення безпеки інформаційних ресурсів у програмно-керованих АТС** 52](#_Toc31009382)

[**2.3.3 Пріоритети забезпечення інформаційної безпеки ЦАТС** 58](#_Toc31009383)

[**2.4 Загальні напрями діяльності щодо забезпечення інформаційної** 59](#_Toc31009384)

[**безпеки ЦАТС** 59](#_Toc31009385)

[**2.4.1 Розробка та впровадження комплексу засобів захисту (КЗЗ) від несанкціонованого доступу (НСД).** 62](#_Toc31009386)

[**2.5 Організація та порядок технічного захисту інформації в ЦАТС** 65](#_Toc31009387)

[**2.5.1 Організація управління інформаційною безпекою** 65](#_Toc31009388)

[2.6 Приклад комплексної системи захисту інформації ЦАТС типу *EWSD* 67](#_Toc31009389)

[**РОЗДІЛ 3.** 76](#_Toc31009390)

[**РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ЗАХИСТУ ІКС НА БАЗІ АТС** 76](#_Toc31009391)

[**3.1 Безпека на фізичному рівні** 76](#_Toc31009392)

[**3.2 БЕЗПЕКА НА СЕРВЕРНОМУ РІВНІ** 77](#_Toc31009393)

[**3.3 Обмеження привілеїв** 77](#_Toc31009394)

[**3.4 Вимкнення сервісів** 79](#_Toc31009395)

[**3.5 Зміна SSH порту** 79](#_Toc31009396)

[**3.5 Безпечне налаштування Asterisk** 80](#_Toc31009397)

[Контекст default 80](#_Toc31009398)

[**3.6 Створення нових директорій для конфігурацій** 81](#_Toc31009399)

[**3.7 Поділ вхідних і вихідних дзвінків** 81](#_Toc31009400)

[**3.8 Використання правил вихідної маршрутизації в ext.conf** 82](#_Toc31009401)

[**3.9 IAX2 аутентифікація** 83](#_Toc31009402)

[**3.10 Одночасне кількість розмов** 85](#_Toc31009403)

[**3.11 Захист Asterisk за допомогою iptables** 86](#_Toc31009404)

[**3.12 Модуль підвищення захисту АТС** 87](#_Toc31009405)

[ВИСНОВОК 93](#_Toc31009406)

[СПИСОК ЛІТЕРАТУРИ 94](#_Toc31009407)

[Додаток А .Захист конфігурацій за допомогою програмного модулю 98](#_Toc31009408)

# **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ**

DLP – Data Loss/Leak Prevention, попередження витоку інформації;

АС – автоматизована система;

БД – база даних;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІР – інформаційні ресурси;

ІС – інформаційна система;

ІТ – інформаційні технології;

ІТС – інформаційно-телекомунікаційна система;

ЗІ – захист інформації;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

ЛОМ – локальна обчислювальна мережа;

НД ТЗІ – нормативний документ технічного захисту інформації;

НСД – несанкціонований доступ;

ОС – обчислювальна система; ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПРД – правила розмежування доступу;

СЗІ – служба захисту інформації;

ТЗ – технічне завдання;

ТЗІ – технічний захист інформації.

# **ВСТУП**

Рівень інформаційної безпеки є важливим критерієм ефективності функціонування для кожного підприємства. Забезпечення потрібного рівня інформаційної безпеки досягається за допомогою застосування різноманітних засобів та заходів, за допомогою створення комплексної системи захисту інформації.

Проблема витоку інформації є дуже актуальною. Великий відсоток витоку здійснюється шляхом порушення політики безпеки, несанкціонованого доступу, навмисного та випадкового. Високий рівень інформаційної безпеки підприємства досягається шляхом розробки ефективної політики безпеки і, як наслідок, оптимальних правил розмежування доступу. Засоби, що реалізують політику безпеки, здійснюють контроль над взаємодією користувачів та інформаційних ресурсів, є ключовою частиною підсистеми керування доступом. Підвищення ефективності роботи цих засобів є важливим завданням.

В даний час поняття АТС стало дуже популярним. Використання IP-АТС обіцяє економію коштів, якість зв'язку і безліч додаткових сервісів. Все більше компаній і просто приватних осіб віддають перевагу послугам IP-телефонії замість традиційної. Однак, стикаючись з реальними системами IP-телефонії на практиці, споживач часто відчуває розчарування. В першу чергу через брак знань через помилки в проектуванні мережі і виборі засобів захисту. Тому, хотілося б чітко окреслити захист АТС.

Проте передача даних цим шляхом не завжди може бути безпечною, тому буде доцільно використовувати віртуальну приватну мережу для шифрування трафіку. Безпека інформації на сьогодні - одна з найважливіших складових роботи системного адміністратора. І чим більша структура підриємства, тим більші можливості з’являються у зловмисників щодо перехоплення інформації, використання ресурсів компанії в своїх цілях.

В роботі розглядаються найбільш поширені вирішення Захисту АТС, одне з яких буде практично реалізовано для досягнення захисту конфігураційних файлів.

**РОЗДІЛ 1.** **ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНО-**

**КОМУНІКАЦІЙНИХ СИСТЕМ**

* 1. ****Сутність та зміст понять у сфері інформаційної безпеки****

Із розвитком інформаційних технологій у всьому світі зростає розуміння переваг, які може надати організаційній структурі інформаційно-комунікаційна система (ІКС). Тому питання створення інформаційно-комунікаційних систем, які б ефективно працювали з інформаційними ресурсами, є надзвичайно актуальним на сьогодні. Під ІКС у загальному випадку розуміється множина сутностей інформатизації та взаємозв’язків між ними.

Згідно чинного законодавства України ІКС – це сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як одне ціле.

Основне призначення інформаційно-комунікаційної системи – забезпечення власне надійної комунікації та обробки інформаційних ресурсів організаційної структури.

Класифікацію ІКС можна проводити за багатьма критеріями. ІКС, які задовольняють інформаційні потреби – інформаційні системи. Такі системи забезпечують доступ користувачів (персоналу, клієнтів, тощо) до інформації. Вони повинні забезпечувати зберігання інформації, пошук, швидкий та захищений доступ.

ІКС, призначені для підтримки бізнес-процесів (інформаційно-аналітичні системи). Прикладом таких бізнес-процесів можуть бути банківські транзакції.

ІКС, призначені для управління організаційною структурою – автоматизовані системи управління. Вони повинні забезпечувати автоматизацію комунікацій, документообігу, контролю за виконанням наказів та розпоряджень, тощо.

Інтелектуалізовані системи, до яких відносяться експертні системи, системи оцінки ефективності та прогнозування результатів управлінських рішень, тощо. Такі системи забезпечують виконання окремих інтелектуальних функцій людини.

У ІКС можна виділити такі складові: апаратне забезпечення; програмне забезпечення; інформаційне забезпечення; організаційне забезпечення; кадрове забезпечення; правове забезпечення.

Слід підкреслити також, що всі ІКС можна поділити на системи міжнародного, державного, рівній, окремих підприємств і організацій чи іх окремих підрозділів.

Структура інформаційно-телекомунікаційної системи типового підприємства зображена на рис. 1.1.

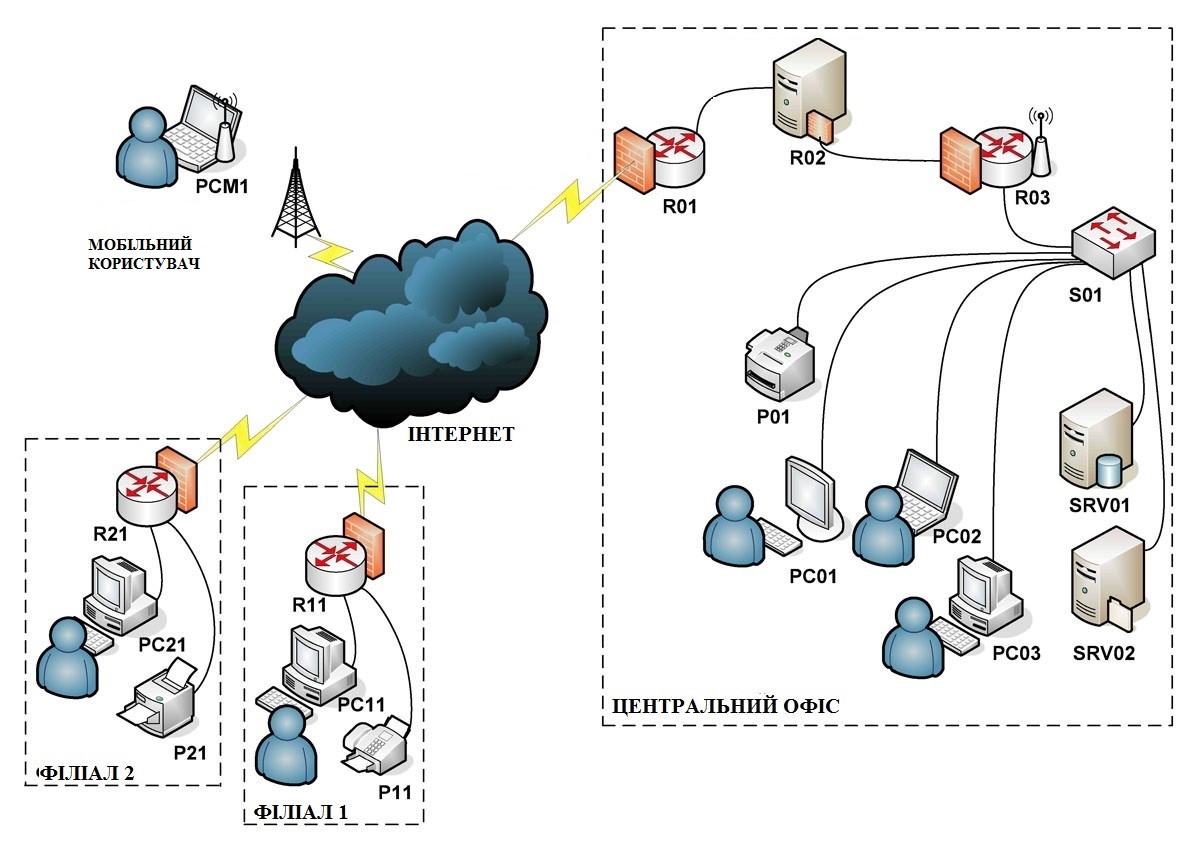


Рис. 1.1. Загальна схема ІТС типового підприємства

ІКС складається із функціональних блоків (підсистем), які з точки зору інформаційної безпеки розглядаються як об’єкти інформаційної діяльності.

Так, наприклад, підсистема контролю доступу і захисту інформації повинна реалізовувати основні методи захисту інформаційних ресурсів від несанкціонованого доступу, а також забезпечувати нейтралізацію випадкових і цілеспрямованих потенційних загроз, таких, що дають змогу порушнику:

* одержувати доступ до даних з порушенням встановлених правил розмежування доступу з метою ознайомлення, модифікації, копіювання, знищення даних і т. ін.;
* зчитувати дані із запам’ятовуючих пристроїв після виконання санкціонованих запитів;
* копіювати носії інформації;
* маскуватися під зареєстрованого користувача, видавати власні несанкціоновані запити за запити операційної системи;
* отримувати захищені дані за допомогою спеціально організованої серії санкціонованих запитів;
* модифікувати програмне забезпечення, навмисно включаючи до його складу спеціальні блоки для порушення безпеки даних;
* фальсифікувати факти формування, видачі та отримання даних;
* підтверджувати отримання від користувача даних, сформованих самим порушником, передачу користувачеві даних, що не передавалися;
* вивчати права доступу інших користувачів;
* незаконно розширювати свої права та змінювати повноваження інших користувачів.

ІКС підприємства, що забезпечує його діяльність та виконання всіх бізнес процесів та задач, є ієрархічною структурою і складається з таких функціональних компонентів [6]:

* робочі станції;
* сервери (файлів, баз даних, служб друку і т. п.);
* мережеві пристрої (маршрутизатори, комутатори, шлюзи, концентратори);
* систем управління базами даних
* засоби зв'язку і передачі даних;
* засоби захисту інформації;
* канали і лінії зв'язку.

Будь-яка ІКС повинна бути не тільки ефективною, а і захищеною від несанкціонованого доступу, витоку інформаційних ресурсів, несанкціонованого доступу тощо, тобто наділеною можливостями забезпечення інформаційної безпеки, що реалізується комплексною системою захисту інформації.

Основною метою системи захисту інформації є:

* фізичне збереження технічних і програмних засобів від викрадення та пошкодження;
* надання користувачам права доступу до ресурсів підсистеми згідно з прийнятою стратегією безпеки;
* забезпечення входу до комп’ютерної підсистеми за умови пред’явлення електронного ідентифікатора або вводу особистого паролю;
* реєстрація дій користувачів щодо ресурсів підсистеми;
* забезпечення цілісності інформаційних ресурсів (у тому числі – забезпечення антивірусного захисту);
* облік носіїв інформації;
* сигналізація про порушення захисту;
* забезпечення цілісності програмних засобів та інформації, що обробляється.

Реалізація комплексу засобів захисту (КЗЗ), основними завданнями якої є ізоляція об'єктів ІКС всередині сфери керування, перевірка всіх запитів доступу до об'єктів і реєстрація запитів і результатів їх перевірки і/або виконання інформації, передбачає виконання низки вимог:

1. Забезпечувати безперервний захист об'єктів. Не повинно існувати можливості одержати доступ до об'єктів ІКС в обхід КЗЗ. КЗЗ має бути безперервно захищеною від злому і несанкціонованої модифікації. Жоден КЗЗ не може вважатись таким, якщо базові апаратні і програмні механізми, що реалізують політику безпеки, самі є суб'єктами для несанкціонованої модифікації або заміни.
2. Мати модульну структуру. На рівні розгляду архітектури ІКС "модульність" означає, що КЗЗ має бути реалізований як набір відносно незалежних частин. Кожна з цих частин повинна взаємодіяти з іншими тільки через добре визначені інтерфейси. На рівні розгляду архітектури КЗЗ "модульність" означає, що КЗЗ має бути спроектовано як набір логічних груп програмного і апаратного забезпечення так, щоб кожна група вирішувала певні завдання.

Так, наприклад, для програмного забезпечення (ПЗ), в простішому випадку під цим слід розуміти, що подібні функції мають бути зосереджені в певних вихідних файлах. Під жорсткішими вимогами слід розуміти використання приховання даних, інкапсуляції та інших механізмів, що дозволяють мати впевненість, що кожний модуль вирішує єдине завдання і що всі дані, якими він оперує, або визначені всередині і доступні як локальні, або передаються як параметри або схожим чином.

1. Будь-яка взаємодія між компонентами повинна здійснюватись тільки через відомі і описані канали (інтерфейси). Оскільки не в усіх випадках це можливо, то за умови забезпечення відповідних гарантій реалізації використання глобальних змінних допускається, хоч і не рекомендується.
2. Посилення вимог до модульності КЗЗ приводить до необхідності побудови КЗЗ відповідно до принципів пошарової архітектури: КЗЗ має бути спроектовано як набір груп функцій (шарів), що взаємодіють тільки з сусідніми нижнім і верхнім шарами [3].
3. Для реалізації політики безпеки КЗЗ повинен забезпечити ізоляцію об'єктів всередині сфери управління і гарантувати розмежування запитів доступу і керування потоками інформації між об'єктами. Для цього з об'єктами КС має бути пов'язана інформація, що дозволяла б КЗЗ ідентифікувати об'єкти і перевіряти легальність запитів доступу. Такою інформація є атрибути доступу[16].
4. Реалізація довірчим і адміністративним доступом. Під довірчим керуванням доступом розуміють таке керування, при якому засоби захисту дозволяють звичайним користувачам управляти потоками інформації між іншими користувачами. Адміністративне керуванням доступом — це таке керування, при якому засоби захисту дозволяють управляти потоками інформації між користувачами і об'єктами тільки спеціально авторизованим користувачам.
5. КЗЗ повинен забезпечувати реєстрацію дій об'єктів-користувачів щодо використання ресурсів системи, а також інших дій і подій, які так або інакше можуть вплинути на дотримання реалізованої КС політики безпеки [19].

### **Аналіз загроз безпеці інформаційних ресурсів**

Під загрозою інформаційній безпеці ІКС різного призначення розуміють будь-які обставини або події, що можуть бути причиною порушення КЗЗ інформації і/або нанесення збитків ІКС.

Загрози інформаційній безпеці є при забезпеченні конфіденційності; доступності; цілісності; спостережності; автентичності; неспростовності; надійності; порядку маршрутизації трафіка.

Конфіденційність порушується крадіжкою (копіюванням) інформації та засобів її обробки; ненавмисною утратою або витом та втратою засобів її обробки.

Доступність – властивість ресурсу системи, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не більше заданого проміжку часу.

Загрози доступності виникають у випадках, коли об'єкт (користувач або процес) не дістає доступу до законно виділених йому служб або ресурсів. Ця загроза реалізується знищенням інформації, блокуванням ліній зв'язку в результаті передачі по ним несанкціонованої інформації або виключенням необхідної системної інформації.

Спотворення інформації, заперечення її справжності, нав’язування хибної інформації спричинює порушення її цілісності.

Спостереженість – властивість ІКС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Автентичність – властивість, яка гарантує, що суб’єкт або ресурс ідентичні заявленим.

Неспростовність характеризується здатністю засвідчувати дію або подію, яка мала місце так, щоб ці події або дії не могли бути пізніше спростовані. (ДСТУ ISO/IEC TR 13335-1:2003 Iнформацiйнi технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції та моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT))

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

* розголошування конфіденційної інформації;
* витік конфіденційної інформації через технічні засоби забезпечення виробничої діяльності різного характеру і виконання;
* несанкціонованого доступу до відомостей, що охороняються, з боку конкурентних організацій і злочинних формувань.
* створення компактних та високоефективних технічних засобів, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації;
* злочинна діяльність, спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;
* відсутність системи атестації на відповідність вимогам ТЗІ об’єктів, робота яких пов’язана з інформацією, що підлягає технічному захисту;
* нелегальне використання ресурсів операторів для несанкціонованого надання послуг зв’язку, що знижує доходи останніх;
* експлуатація різних фрагментів мережі різними операторами з різними формами власності.

Здійснення загроз інформаційним ресурсам може бути проведене:

* шляхом неофіційного доступу і знімання конфіденційної інформації, підкупу осіб, що працюють;
* шляхом перехоплення інформації, циркулюючої в засобах і системах зв'язку і обчислювальної техніки, несанкціонованого доступу до інформації і навмисних програмно-математичних дій на неї в процесі обробки і зберігання;
* шляхом підслуховування конфіденційних переговорів, що ведуться в службових приміщеннях, службовому і особистому автотранспорті тощо;
* через переговорні процеси між підприємством і іноземними або вітчизняними фірмами, використовуючи необережне поводження з інформацією;
* через окремих співробітників підприємства, які мають корисливу або особисту зацікавленість.

Узагальнення можливихі шляхів реалізації загроз безпеки для де-яких обʼєктів атаки наведені в табл. 1.1.

Джерела загроз інформаційній безпеці традиційно поділяють на три групи на антропогенні джерела (зумовлені зловмисними чи випадковими діями суб’єкта)); техногенні джерела (зумовлені технічними засобами); природні джерела (зумовлені природними стихійними джерелами).

До 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.

Внутрішніми антропогенними джерела загроз є основний персонал; системні і мережні адміністратори, адміністратори безпеки; керівництво; технічний персонал і допоміжний персонал; співробітники, звільнені з роботи; особи з порушеною психікою, впроваджені та завербовані агенти з числа основного, допоміжного та технічного персоналу, представників служби захисту інформації.

Техногенні джерела загроз також поділяють на зовнішні та внутрішні техногенні джерела загроз, серед яких відначимо такі: засоби службового зв’язку; мережі водопостачання, каналізації, вентиляції; засоби пожежної, охоронної сигналізації; транспорт; технічні і програмні засоби комутації, обробки інформації; засоби управління.

*Таблиця 1.1*

Шляхи реалізації загроз безпеки

|  |  |  |  |
| --- | --- | --- | --- |
| Обʼєкти  впливу | Порушення  конфіденційності  інформації | Порушення  цілостності  інформації | Порушення  працездатності  системи |
| Апаратні  засоби | Несанкціоновані підключення та використання ресурсів; розкрадання носіїв | Несанкціоновані підключення та використання ресурсів; модифікація, зміна  режимів | Несанкціонована зміна режимів; руйнування |
| Програмне  забезпечення | Несанкціоноване копіювання; викрадення | Несанкціонований доступ; засилання вирусів | Спотворення; видалення; підміна |
| Дані | Несанкціоноване копіювання; викрадення; перехоплення | Спотворення; модифікація | Спотворення; видалення; підміна |
| Персонал | Розголошення; передача відомостей про захист; недба- лість | Вербування, підкуп персоналу | Залишення робочого місця без нагляду, фізичне усунення працівника |

Але поряд з цим загрози можна класифікувати і за іншими ознаками: за мета; за принцип та характер впливу на ІКС; спосіб впливу на обʼєкт атаки; спосіб дій порушника; використання засобів атаки; обʼєкт атаки.

За оцінкою вітчизняних і зарубіжних дослідників персонал є важливим внутрішнім джерелом ризику ухвалення помилкових рішень і протиправної поведінки, у тому числі і у зв'язку з діями інших осіб і організацій з примусу співробітників до злочинної діяльності. При цьому можливі спроби впровадження в кадровий склад представників кримінальних і інших недружніх підприємству організацій.

У цьому сенсі доречно розрізняти:

− загрози, пов'язані з навмисними або ненавмисними діями осіб, що мають доступ до ІКС, включаючи користувачів, що реалізовують погрози безпосередньо в ІКС (внутрішній порушник);

− загрози, пов'язані з навмисними або ненавмисними діями осіб, що не мають доступу до ІКС і реалізовують погрози з зовнішніх мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну (зовнішній порушник).

Оцінки ступеня реалізації загроз інформаційним ресурсам від ненавмисних дій персоналу наведені в табл. 1.2, а навмисних – в табл. 1.3.

*Таблиця 1.2.*

Аналіз ступеня реалізації загроз інформаційним ресурсам ІКС від

ненавмисних дій персоналу

|  |  |  |  |
| --- | --- | --- | --- |
|  | Ступінь реалізації | | |
| Вид загрози | Висока | Середня | Низька |
| Помилка персоналу | + |  |  |
| Порушення експлуатації технічних засобів |  | + |  |
| Несанкціоноване використання обладнання |  | + |  |
| Помилки при обробці інформації |  | + |  |
| Втрати ключів доступу | + |  |  |
| Зміна інформації | + |  |  |
| Відключення засобів захисту |  |  | + |

Узагальнене подання інформації про види та джерела загроз ІБ, методи реалізації та захисту, а також наслідки зображено на рис. 1.2 [22].



Рис. 1.2. Модель реалізації загроз

## **1.14 Висновки**

1. Визначення протидії загрозам безпеки в інформаційних системах становить комплексну проблему, для вирішення якої необхідно поєднання заходів на законодавчому, адміністративному, процедурному і програмно-технічного рівнів ІБ.
2. Розробка та прийняття нормативно-правових актів у галузі захисту інформації покликані врегулювати безпечне використання інформаційно-комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу та витоку технічними каналами.
3. Призначення адміністративного рівня протидії загрозам інформаційної безпеки має зводитися до таких важливих практичних кроків як визначення керівних документів і стандартів, підходів до управління ризиками та сертифікація на відповідність стандартам інформаційної безпеки.

## **РОЗДІЛ 2. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

## **ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ**

# **2.1. Загальна характеристика засобів та методів захисту інформаційних ресурсів**

Основними завданнями засобів захисту є ізоляція об'єктів ІКС всередині сфери керування, перевірка всіх запитів доступу до об'єктів і реєстрація запитів і результатів їх перевірки і/або виконання. З одного боку, будь-яка елементарна функція будь-якої з послуг, що реалізуються засобами захисту, може бути віднесена до функцій ізоляції, перевірки або реєстрації. З іншого боку, будь-яка з функцій, що реалізуються засобами захисту, може бути віднесена до функцій забезпечення конфіденційності, цілісності і доступності інформації або керованості КС і спостережностi дій користувачів.

Кожна функція може бути реалізована одним або більше внутрішніми механізмами, що залежать від конкретної ІКС. Реалізація механізмів може бути абсолютно різною. Вибір методів і механізмів практично завжди залишається за розробником. Єдиною вимогою залишається те, щоб функції захисту були реалізовані відповідно до декларованої політики безпеки і вимог гарантій.

Для забезпечення захисту інформаційних ресурсів у ІКС застосовується низка організаційних, інженерно-технічних, програмних засобів та методів.

**Організаційні заходи** є обов’язковою складовою побудови будь-якої КСЗІ і не вимагають великих матеріальних витрат, але їх ефективність підтверджена життям і часто недооцінюється потенційними зловмисниками. Особливою ознакою організаційних заходів є те, що вони застосовуються до зіткнення зі зловмисником і ніколи не стають провокуючим фактором агресії.

Використовуючи досвід багатьох організацій в області проектування КСЗІ, можна сказати, що організаційні заходи включають в себе створення концепції інформаційної безпеки. Вони включають:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;

- створення правил адміністрування, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

- розробку планів дій у разі виявлення спроби несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайних ситуацій;

- навчання правилам інформаційної безпеки користувачів;

- дотримання основних принципів, простих правил і інструкцій, що дозволить запобігти втраті інформації, можливим матеріальним і фінансовим втратам тощо.

**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, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання захисту від несанкціонованого доступу. У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом. Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної інформації.

Особливим, ефективним та поширеним видом інженерно-технічних заходів є криптографічні засоби захисту інформації. Захист даних за допомогоюшифрування – одне з можливих рішень проблеми їхньої безпеки. Зашифровані дані стають доступними тільки для того, хто знає, як їх розшифрувати.

Коди і шифри використовувались задовго до появи ЕОМ. З теоретичного погляду не існує чіткої різниці між кодами і шифрами. Однак у сучасній практиці відмінність між ними, як правило, є достатньо чіткою. Коди оперують лінгвістичними елементами, поділяючи текст, що шифрується, на такі смислові елементи, як слова і склади. У шифрі завжди розрізняють два елементи: алгоритм і ключ.

Зашифровування даних називається процес перетворення відкритих даних на шифровані з допомогою шифру, а розшифруванням даних – процес перетворення закритих даних на відкриті з допомогою шифру. Дешифруванням будемо називати процес перетворення закритих даних на відкриті при невідомому ключі і, можливо, невідомому алгоритмі.

Криптографічний захист – це захист даних з допомогою криптографічного перетворення, під яким розуміється перетворення даних шифруванням і (або) виробленням імітовставки, що являє собою послідовність даних фіксованої довжини, отриману за певним правилом з відкритих даних і ключа.

Ключовою характеристикою шифру є його криптостійкість, тобто його стійкість до дешифрування. Звичайно ця характеристика визначається періодом часу, необхідним для дешифрування.

Вимоги до методів шифрування даних визначаються криптографічними стандартами.

Одним з найбільш розповсюджених криптографічних стандартів на шифрування даних, що застосовуються в США, є DES (Data Encryption Standard). Первісно засіб, що лежить в основі даного стандарту, був розроблений фірмою IBM для своїх цілей. Він був перевірений Агенцією Національної Безпеки США, що не виявило в ньому статистичних або математичних вад. Це означало, що дешифрування даних, захищених з допомогою DES, не могло бути виконане статистичними (наприклад, з допомогою частотного словника) або математичними ("прокручуванням" в зворотному напрямку) засобами.

Засіб DES може бути реалізований і програмно. Залежно від швидкодії та типу процесора персонального комп'ютера програмна система, що шифрує дані з використанням засобу DES, характеризується низькою швидкодією і може обробляти від декількох кілобайт до десятків кілобайт даних у секунду. У той же час необхідно відзначити, що базовий алгоритм все ж розрахований на реалізацію в електронних приладах спеціального призначення.

Вдосконаленою версія DES стандарту є TripleDES (3DES). Він допускає триразове використання первинного DES для на даних у три фази: шифрування, дешифрування та знову шифрування і забезпечує ефективну довжину ключа у 168 біт, на відміну від звичайного DES.

Стандарти шифруванняAES **(**Advanced Encryption Standart - розширений стандарт шифрування) регламентує симетричний блок-шифр і підмножину шифру Рінддейла. AES використовується у всьому світі для захисту секретної інформації та шифрування конфіденційних даних у програмному та апаратному забезпеченні.

Стандартом AES передбачено застосування трьох різних блок-шифрів: AES-128; AES-192; AES-256.

У шифрі Рінддейла, на відміну від АЕS, є додаткові розміри блоків і ключових розмірів, але шифр AES цих функцій не реалізував.

Розмір ключа означає кількість бітів у ключі. Короткі ключі можуть бути вразливими для грубої атаки (наприклад, методом перебору).

Практичним застосуванням криптографічних стандартів є низка методів та алгоритмів, що реалізуються певними програмами, протоколами та цифровими сертифікатами.

Серед поширених протоколів шифрування відзначимо протокол IPSec, протокол тунелювання "точка-точка" (англ. Point-to-Point Tunneling Protocol – PPTP), протокол L2TP (Layer Two Tunneling Protocol - протокол тунелювання другого рівня), протокол SSL (Secure Socket Layer).

Базовий протокол IP є не дуже захищеним та забезпечує жодної автентифікації та конфіденційності. Новий стандарт IPv6 позбавлений цього недоліку і використовуює 128-бітну адресу.

Повна реалізація стандарту IPv6 потребує широкого оновлення обладнання. Розроблена реалізація безпеки IPsec не потребує великих змін у схемі адресації і може бути реалізований різними алгоритми

Цифрові сертифікати використовують комбінацію типів шифрування для забезпечення автентифікації, тобто для підтвердження істинності відправника інформації. Сертифікати зазвичай видаються органом з сертифікації або створюються та підписуються локально.

Серед програм шифрування відзначимо Хеш-програму, яка реалізує спеціальні односторонні функції для забезпечення автентифікації та перевірки. Найпопулярнішим алгоритмом хешування є MD5 [57].

Тепер зупинимося на засобі RSA. Він є дуже перспективним, оскільки для зашифровування інформації не вимагається передачі ключа іншим користувачам. Це вигідно відрізняє його від всіх описаних вище засобів криптографічного захисту даних. Але в наш час до цього засобу відносяться з підозрою, оскільки в ході подальшого розвитку може бути знайдений ефективний алгоритм визначення дільників цілих чисел, в результаті чого засіб шифрування стане абсолютно незахищеним. Крім того, не має чіткого доказу, що не існує іншого засобу визначення таємного ключа за відомим, окрім як визначення дільників цілих чисел.

У решті-решт, засіб RSA має лише переваги. До числа цих переваг слід віднести дуже високу криптостійкість, досить просту програмну і апаратну реалізації. Щоправда, слід помітити, що використання цього зІКСобу для криптографічного захисту даних нерозривно пов'язане з дуже високим рівнем розвитку техніки.

Сучасні системи захисту інформаційних ресурсів ІКС реалізуються, зазвичай, на основі DLP (Data Leak/Loss/Leakage Prevention) – технології, яка запобігає витокам конфіденційної інформації за межі ІКС. При виявленні в потоці даних конфіденційної інформації активна компонента DLP-системи блокує передачу повідомлення.

DLP-системи проводять глибокий аналіз змісту інформації та її категоріювання, організовують автоматичний захист конфіденційних даних у кінцевих інформаційних ресурсах, на рівні шлюзів передачі даних і в системах статичного зберігання даних, запускають процедуру реагування на інциденти.

DLP-система забезпечує контроль над переміщенням інформації як на рівні комунікацій з зовнішньою мережею, так і на рівні кінцевих пристроїв користувачів (рис. 2.1.).

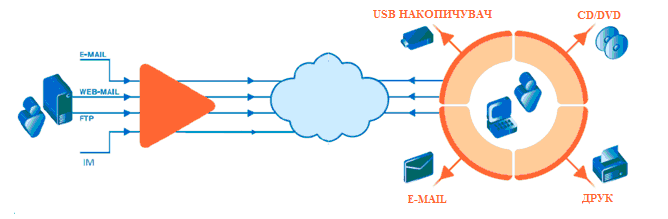


Рис. 2.1. Контрольовані DLP-системою іформаційні потоки [16]

### **2.2.** **Забезпечення інформаційної безпеки інформаційно-комунікаційних систем на основі DLP-технології**

Як зазначалось, DLP-система – це засіб, який дає змогу виявити і блокувати несанкціоновану передачу конфіденційної інформації (її витік) з будь-якого електронного каналу комунікації, використовуючи інформаційну інфраструктуру підприємства.

У якості таких контрольованих каналів можуть виступати Інтернет-пейджери, веб-пошта, соціальні мережі, блоги, форуми, файлообмінники, FTP, пірингові мережі, сервіси відправки SMS, програми для обміну миттєвими повідомленнями, зовнішні пристрої, підключені до робочих станцій або серверів (USBдиски, CD/DVD, локальні принтери, несанкціоновані передавачі WiFi, Bluetooth, модеми тощо).

DLP-система повинна забезпечити можливість виявити випадкове або навмисне несанкціоноване використання інформації співробітниками компанії, а не перекривати повністю всі канали. Сучасні DLP-рішення дають змогує здійснювати перехоплення мережевого трафіку і, на підставі бази алгоритмів і сигнатур, відновлювати передані повідомлення.

Незважаючи на те, що кожен розробник DLP-системи пропонує свою власну архітектуру, в її структурі обов’язковими є такі модулі: центральний керуючий сервер; перехоплювачі / контролери на різні канали передачі інформації; - програми, що встановлюються на кінцеві пристрої (див. рис.2.1).

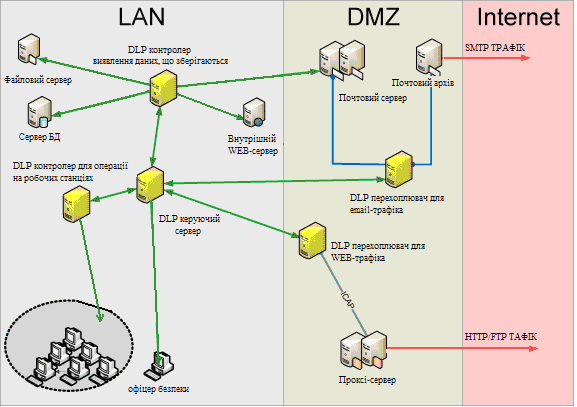


Рис. 2.2 Типова архітектура побудови DLP-системи [16]

Перехоплювачі аналізують потоки інформації, яка може бути виведена за периметри компанії, виявляють конфіденційні дані, класифікують інформацію і передають для обробки можливого інциденту на керуючий сервер. Перехоплювачі можуть бути як для копії вихідного трафіку, так і для установки в розрив трафіку. В останньому випадку потенційний витік може бути зупинений системою DLP.

Контролери для виявлення даних, що зберігаються, запускають процеси виявленнях в мережевих ресурсах конфіденційної інформації. Способи запуску виявлення можуть бути різними: від власне сканування від сервера, контролера до запуску окремих програмних агентів на існуючі сервери або робочі станції [11].

Контролери для операцій на робочих станціях розподіляють політику безпеки на кінцеві пристрої, аналізують результати діяльності співробітників з конфіденційною інформацією і передають дані можливого інциденту на керуючий сервер.

Агентські програми на кінцевих робочих місцях помічають конфіденційні дані в обробці і стежать за дотриманням таких правил, як збереження на змінний носій інформації, відправлення, роздрукування, копіювання через буфер обміну.

Керуючий сервер забезпечує: об’єднання компонентів в єдину систему; визначення даних, що містять конфіденційну інформацію; створення, редагування і розповсюдження політик роботи з конфіденційними даними; збір, зберігання і обробку інцидентів, створення і розсилку звітів; надання ролевого доступу до управління системою співробітникам служби інформаційній безпеці.

Модулі моніторингу і блокування конфіденційної інформації, що передається по мережевих каналах. Вони можуть бути представлені як одним пристроєм, що реалізовує обидві функції, так і окремими (наприклад, Network Monitor, Network Prevent for Web, Network Prevent for E-mail) [3].

Скануючий модуль – це додатковий компонент, який допоможе визначити місцезнаходження конфіденційної інформації в мереж підприємства. За допомогою цього модуля виконується сканування робочих станцій співробітників, файлових серверів, баз даних і так далі. Після завершення процесу виводиться детальний звіт по кожному комп’ютеру або каталогу із загальним доступом. Крім того, такий модуль зможе переміщувати знайдену конфіденційну інформацію з робочих станцій співробітників, каталогів із загальним доступом і інших ресурсів в місце, задане адміністратором. Тобто, даний модуль не тільки оптимізує роботу адміністратора, але і упорядковує зберігання даних на серверах компанії [3].

Мережевий модуль аналізує повний обсяг вихідного трафіку підприємства. Саме завдяки цьому компоненту співробітники відділу ІТ-безпеки можуть контролювати, яка інформація «витікає» за межі корпоративної мережі. Мережевий модуль виконує не тільки аудит витоків конфіденційної інформації, але і здатний заблокувати подібні спроби.

Агенти для робочих станцій і серверів забезпечують контроль переміщення конфіденційних даних на змінні носії інформації (USB, CD/DVD і ін.); переміщення даних до буферу обміну; дій, які співробітник виконує з конфіденційною інформацією, виконують функцію пошуку конфіденційних даних на локальних дисках.

Захист конфіденційної інформації в DLP-системі здійснюється на трьох рівнях потоків даних:

* дані, які передаються по мережевих каналах (Data-in-Motion), зокрема Web (HTTP/HTTPS протоколи); Інтернет–меседжери (ICQ, QIP, Skype, MSN, WhatsUpp, Telegram); корпоративна і особиста пошта (POP, SMTP, IMAP); безпровідні системи (WiFi, Bluetooth, 3G тощо); FTP – з’єднання;
* дані, що статично зберігаються (Data-at-Rest) на серверах; робочих станціях; ноутбуках; системах зберігання даних (СЗД);
* дані, які використовуються на робочих станціях (Data-in-Use).

Для розуміння особливостей будь-якої системи, у тому числі і DLP, застосовують їх класифікацію за різними класифікаційними ознаками.

Так, залежно від архітектури побудови і умов функціонування сучасні DLP-системи поділяють на агентські, периметрові та гібридні.

До агентських відносять системи, модулі яких встановлюються на робочі станції і несуть у собі базову функціональність захисту від витоків на рівні робочої станції.

Периметрові системи встановлюються в розрив каналу. Також до даного класу можна віднести системи, які інтегруються в компоненти інфраструктури (поштові сервери, web-сервери, сервера друку тощо) на рівні відповідних плагінів до них і забезпечують функціональність засобів захисту від витоків на мережевому рівні.

Гібридні є певною комбінацією периметрових і агентських систем.

За іншою ознакою - реакцією на загрозу конфіденційності - умовно всі DLP-системи можна розділити на активні, пасивні і комбіновані.

Пасивні DLP-системи – це системи розслідування інцидентів, що відбулися. Дані системи не блокують витік інформації, але здатні надати вичерпні відомості про джерело і канали витоку. Такі системи складаються з перехоплювачів сніфферів, що копіюють всі електронні повідомлення, які відправляються по основних каналах комунікації: корпоративною і Web-поштою, соціальним мережам, IM, FTP, принтерам і USB-носіям.

Активні DLP-системи забезпечують блокування витоку конфіденційної інформації в режимі реального часу шляхом контролю переміщення конфіденційної інформації всіма основними каналами комунікації.

Режим таких систем не обмежується режимом блокування, а доповнюється і режимом моніторингу. У таких систем, як правило, відсутній повноцінний архів і не можна відновити все листування співробітників при розслідуванні.

Комбіновані DLP-системи необхідні при одночасній архівації всіх електронних повідомлень для подальшого розслідування і блокуванні витоку конфіденційних даних через основні канали комунікацій.

У сучасних DLP-системах зазвичай реалізовано три методи ідентифікації: імовірнісний, детерміністський і комбінований. Системи, засновані на першому методі, здебільшого використовують лінгвістичний аналіз контента і «цифрові відбитки» даних. Такі системи прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових спрацьовувань.

Системи зорієнтовані на детермінований підхід (мітки файлів), дуже надійні, але їм не вистачає гнучкості. Комбінований підхід поєднує обидва методи з аудитом середовища зберігання і обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації [2].

У DLP-системах застосовуються складні механізми аналізу: порівняння по шаблонах з використанням словників і регулярних виразів, лінгвістичний і контекстний аналіз, цифрові відбитки.

У лінгвістичному і контекстному аналізі використовуються морфологія і статистичні моделі, враховується контекст, характер відправника і одержувача інформації. Цей метод хороший для динамічних даних. Цифрові відбитки (аналогічні сигнатурам в антивірусних продуктах) підходять для контролю статичних даних, наприклад, для захисту інтелектуальної власності.

Методом аналізу є пошук в потоці даних деякої послідовності символів («стоп-слів»). У переважній більшості випадків сигнатурні системи налаштовані на пошук декількох слів і частоту зустрічальності термінів.

Метод аналізу масок є розширенням функціонала пошуку сигнатур і є пошуком такого змісту, який неможливо точно вказати в базі "стоп-слів", але можна вказати його елемент або структуру.

Лінгвістичний метод аналізу тексту несе на собі характеристику всього класу методів аналізу вмісту. Технологія лінгвістичного аналізу дозволяє автоматично визначати тематику і ступінь конфіденційності аналізованого фрагмента інформації на підставі термінів, що зустрічаються в ньому, і їх поєднань. Лінгвістичний аналіз виконується на основі заздалегідь створеної бази контентної фільтрації (БКФ).

БКФ не тільки описує категорії інформації, яка циркулює в компанії, але і враховує різні атрибути її конфіденційності, у тому числі специфіку діяльності компанії, її вимоги до безпеки [18].

БКФ визначає надійність і точність ідентифікації конфіденційних даних в корпоративних інформаційних потоках за допомогою технології лінгвістичного аналізу. Основним методом лінгвістичного аналізу за допомогою БКФ є пошук в аналізованому фрагменті інформації слів і словосполучень, що описують конфіденційні дані і структурованих за категоріями.

## **РОЗДІЛ 3.** **РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ**

## **ЗАХИСТУ ЦИФРОВОГО ПРОГРАМНО КЕРОВАНОГО**

## **КОМУТАЦІЙНОГО ВУЗЛА ІКС**

Інформаційно-комунікаційні системи, як зазначалось, складається із низки функціональних підсистем, що забезпечують реалізацію всіх видів діяльності підприємств, організацій, органів управління тощо. До числа таких об’єктів інформаційної діяльності відносяться і різні підсистеми комунікації, зокрема такі, як цифрові програно керовані автоматичні телефонні станції (ЦАТС).

Забезпечення інформаційної безпеки таких телекомунікайних підрозділів підприємств та організацій, які хоча і є допоміжними, включає реалізацію та підтримку процесу проектування, комплексної системи інформаційної безпеки, процесу створення , функціонування та вдосконалення системи інформаційної безпеки та процесу управління ІБ.

### **3.1. Цифровий вузол комутації**

Для надання послуг якісного, надійного, безпечного телефонного зв’язку має бути сформована надійна захищена інфраструктура ЦАТС та ліній телекомунікацій із 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:

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

Узагальненамодельінфраструктурицифровоговузлукомутаціїз позицій технічного захисту інформації показана на рис. 3.1.

У структурі ЦАТС зазвичай виділяють станційну частину, блоки абонентських виносів (БАВ) і мережу абонентських, з’єднувальних та міжстанційних цифрових та аналогових ліній. Такі лінії для порушника є об’єктами несанкціонованого доступу до них, до інформації, що ними передається, і впливу на їх працездатність. На лініях може бути несанкціоновано встановлено обладнання.

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

У якості міжстанційних з’єднувальних ліній можуть використовуватись цифрові канали Е1 з магістральної мережі *SDH* чи АТМ.

Станційна частина цифрового вузла комутації містить у своєму складі:

* підсистему комутації абонентських і з’єднувальних ліній;
* управляючий комплекс вузла комутації з автоматизованими робочими місцями операторів (АРМ оператора);
* підсистему технічної експлуатації 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:

* автоматизована система контролю та розрахунків з абонентами для тарифікації наданих телефонних послуг (АСКР);
* *TMN* – мережа управління електрозв’язком для технологічного контролю та адміністративно-бізнесового менеджменту послуг;
* *IN* – мережа надання інтелектуальних послуг;
* *SS*7 – система сигналізації для управління процесом з’єднання;
* СС - система синхронізації для отримання опорних тактових частот.

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

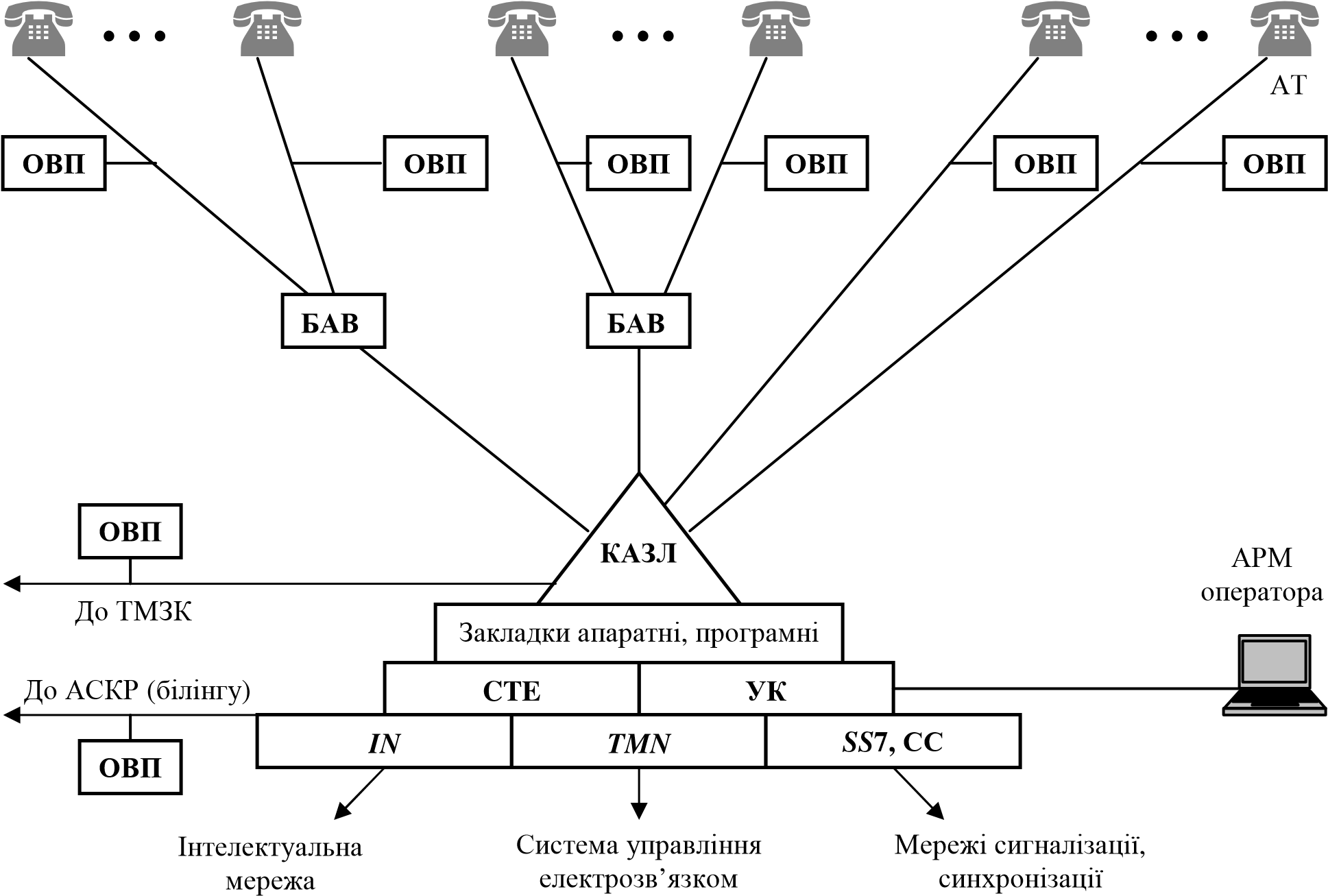


Рис. 3.1. Функціональна схема цифрового вузла комутації

На рис. 3.1 застосовані такі позначення: АТ – абонентські термінали; БАВ – блок абонентського виносу; КАЗЛ – підсистема комутації абонентських та з’єднувальних ліній; ОВП - обладнання, встановлене порушниками; СТЕ – система технічної експлуатації; ТМЗК – телекомунікаційна мережа загального користування; УК – управляючий комплекс.

Структурнасхемастанційноїчастиницифрової програмно*-*керованоїАТСзпозиційтехнічного захисту інформації (ТЗІ) відповідно до НД ТЗІ 1.1-001-99 наведена на рис. 3.2.

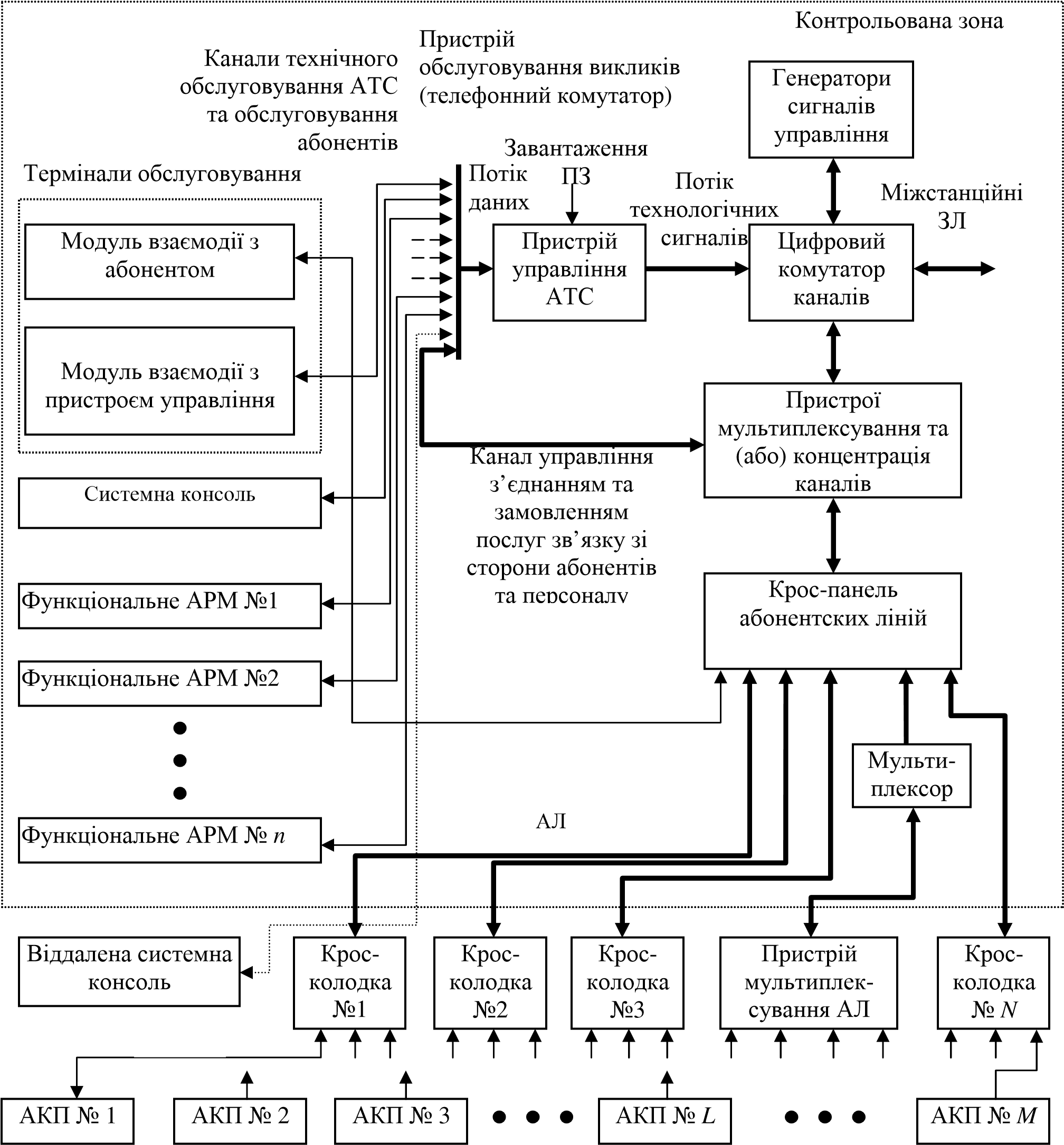


Рисунок 2.2 – Структурна схема станційної частини програмно-керованої АТС з позицій ТЗІ (з НД ТЗІ 1.1-001-99)

На схемі використані такі 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.

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

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

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

У структурі підсистема управління станцією передбачається спеціалізовані пристрої управління, що реалізують принцип програмного управління. Такими пристроями, здебільшого є процесори, пристрої внутрішньої і зовнішньої пам’яті, периферійні пристроїв, спеціалізовані модулі управління сигналізацією, опрацювання викликів, надання послуг і деяких інших програмно-апаратних компонентів, а також термінали обслуговування, що приєднані до пристроїв управління через канали технологічного обслуговування АТС і до підсистеми КАЗЛ - через канали інформаційного обслуговування абонентів.

Пристрої, що реалізують процеси комутації, мультиплексування та концентрації абонентських і міжстанційних з’єднувальних ліній, а також компоненти устаткування абонентських ліній зв’язку - абонентські прикінцеві пристрої, фізичні лінії зв’язку, пристрої мультиплексування абонентських ліній, станційні абонентські комплекти тощо є складовими підсистема КАЗЛ.

Незалежність підсистем управління станцією і КАЗЛ визначається тим, що підмножина загроз для інформації, яка характерна для підсистеми управління станцією, не перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ.

Коректність такої декомпозиції структури програмно-керованих АТС обумовлена прийнятими щодо них проектними рішеннями.

## **3.2 Особливості загроз інформаційним ресурсам вузла комутації**

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

* комунікаційне обладнання, яке використане у мережах зв’язку;
* прогресу 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.;
* злочинна діяльність, спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним чи фізичним особам;
* 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;
* 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.
* 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].

Класифікацію моделей порушників антропогенного типу, їх рівні можливостей, основні способи реалізації загроз для інформації програмнокерованих АТС наведено у НД ТЗІ 1.1.001-99 [8]. Виділено чотири рівні можливостей порушення НСД:

1. Запуск програм (задач) із фіксованого набору, котрий реалізує передбачені функції щодо обробки інформації. До цього причетні обслуговуючий персонал, який забезпечує експлуатацію обладнання ЦАТС, зокрема інженери-електронники ЦАТС.
2. Можливість створення та запускання власних програм із новими функціями щодо обробки інформації.
3. Можливість впливу на базове ПЗ ЦАТС та на склад і конфігурацію обладнання. Такими можливостями наділені оператори ЦАТС. Типові можливості такого порушника: формування штатних команд, запускання задач, не задекларованих у технічній документації, несанкціоноване приєднання до інформаційних трактів.
4. Обсяг усіх можливостей суб’єктів, здійснюючих проектування, реалізацію та ремонт технічних засобів, до залучення у склад обладнання власних технічних засобів з новими функціями. Це програмісти, котрі беруть участь у розробленні й виготовленні вузлів комутації. Типові можливості є такі: впровадження програмних закладок, впровадження шкідливих кодів (вірусів), помилки у ПЗ та комутаційній системі.

Загрози інформаційній безпеці ЦАТС можуть бути різноманітними і довільного походження за часом, тривалістю, факторами та наслідками. Вихід із ладу ЦАТС можливий при зупинці системи електроживлення або виведенні її з ладу порушником. До розглядуваних загроз можна віднести можливе впровадження “вірусу” – мікропрограми, здатної самостійно розмножуватись і поширюватись у мережі.

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 немає, то можливі впливи порушника через зовнішні інтерфейси обладнання, системи сигналізації на абонентських та з’єднувальних лініях.

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

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

У межах контрольованої зони ЦАТС може встановлюватись різноманітне устаткування телекомунікаційних мереж. Частина цього обладнання приєднується безпосередньо до обладнання ЦАТС і може впливати на її роботу. Зокрема, це система сигналізації й синхронізації, система централізованого управління та технічної експлуатації, з’єднувальні та абонентські лінії, системи передавання до АСКР тощо.

До можливихваріантівінформаційногонападунамережізв*’*язку відноять такі загрози:

* загроза атаки через АРМ адміністратора;
* загроза несанкціонованого входу в АРМ адміністратора;
* загроза модифікації апаратної частини АРМ, АТС, *SS*7 і лінійної апаратури (вставка чужого пристрою);
* загроза відмови в обслуговуванні;
* 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.

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. 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.

Застосування сигналізації *SS*7 дозволяє здійснювати певні функції управління окремими вузлами зв’язку, при якому може бути нанесена значна шкода оператором зв’язку. Системи сигналізації забезпечують передавання різноманітних сигналів управління, в тому числі цифр номера, які через функціональні елементи комутаційної системи надходять для аналізу в управляючий комплекс.

У складі *SS*7 є підсистеми забезпечення можливостей транзакцій (*TCAP*) та прикладних підсистем, котрі організуються на них, такі як підсистема рухомого зв’язку *GSM* (*MAP*), підсистема інтелектуальних мереж (І*NAP*), підсистема експлуатації, техобслуговування, адміністрування й управління (*OMAP*) та інші. До загроз від застосування *SS*7 також належать:

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

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

Здійснювати НСД може порушник з правами оператора шляхом формування штатних команд, запускати програми, нерегламентовані в технічній документації.

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 ПК і використовують для роботи операційну систему *Windows* чи *MS-DOS*.

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

На ІБ інформаційних ресурсів ЦАТС впливають і агрозинаабонентськихтаз*’*єднувальнихлініях, вцифровихсистемахпередачі. Останні мають вразливості на фізичному, канальному та мережному рівнях стеку протоколів передавання.

На фізичному рівні порушник прагне НСД через консолі управління або активізацією “закладок”, впроваджених в об’єктах цифрових систем передавання.

На канальному рівні порушник може виконувати дії на активізацію вразливості відповідних протоколів. Порушник може одержати доступ до інформації, активізувати “закладку” формуванням спеціальних команд в кадрах (комірках, контейнерах) даних.

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

# **3.3 Мета, принципи діяльності та пріоритети забезпечення інформаційної безпеки ЦАТС**

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

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

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

Центри комутації та їх виноси розташовані на невеликих територіях і захищаються методом “кругової оборони” (бар’єрним методом).

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

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

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

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

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

Основними принципами діяльності щодо інформаційної безпеки є такі:

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

мають здійснюватись зміни пріоритетів в діяльності щодо ТЗІ та відповідні зміни стратегій забезпечення безпеки;

* безперервності – заходи щодо ТЗІ здійснюються на всіх технологічних етапах надання послуг зв’язку;
* сумісності та безконфліктності засобів захисту;
* систематичності – постійний аналіз загроз, що мають суттєве значення для користувачів та відповідне попереджуюче впровадження засобів протидії цим загрозам в тій мірі, за якої витрати на протидію загрозам не перевищують збитків від їх здійснення;
* збереження якісних показників – технічні та програмні засоби, що використовуються для забезпечення ТЗІ, не повинні суттєво погіршувати основні технічні показники засобів та систем зв’язку;
* контрольованості - наявність можливості моніторингу ефективності заходів щодо ТЗІ;
* керованості в залежності від вимог до захищеності інформації та мінімізації витрат. Має створюватись система управління комплексами засобів захисту, що дозволяє здійснити безперервний контроль ефективності засобів захисту та підтримку необхідного рівня захищеності інформаційних ресурсів ЦАТС;
* масштабованості – можливість легкого нарощування КСЗІ одночасно з розширенням ємності ЦАТС;
* адекватності заходів захисту інформації реальним та потенційним загрозам.

Пріоритети ранжуються у залежності від важливості інформації та мінімізації збитків відповідно за напрямами забезпечення інформаційної безпеки:

* для забезпечення керованості системи інформаційної безпеки, в залежності від вимог до захищеності інформації та мінімізації витрат, має створюватись системауправлінняінформаційноюбезпекою та комплексами засобів захисту, що дозволить здійснити необхідний безперервний контроль ефективності засобів захисту, підтримку необхідного рівня захищеності інформаційних ресурсів ЦАТС;
* 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;
* запровадити систему управління інформаційною безпекою у всіх підрозділах підприємства.
* збільшення пріоритету захисту відкритої інформації. 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.

## **3.4. 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.

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

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

* загальні положення з управління інформаційною безпекою: політика безпеки; організація захисту; класифікація ресурсів та їхній контроль;
* безпека персоналу, фізична безпека й безпека навколишнього середовища;
* адміністрування комп’ютерних систем та обчислювальних мереж;
* управління доступом до систем;
* розробляння й супроводження інформаційних систем; 6) планування захисту: планування безперебійної роботи підприємства;
* виконання вимог.

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

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

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

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

Оцінка ризику залежить від таких чинників:

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

Успішне здійснення системи інформаційної безпеки визначається таким:

* + забезпечування безпеки має ґрунтуватися на виробничих цілях і вимогах;
  + функції управління безпекою має взяти на себе керівництво підприємства;
  + оцінювання ризиків порушування безпеки, загроз і слабкостей інформаційних ресурсів та рівня їхньої захищеності має ґрунтуватися на цінності й важливості цих ресурсів;
  + ознайомлення з системою безпеки всіх керівників та рядових співробітників підприємства;
  + вивчання співробітниками політики та стандартів інформаційної безпеки;
  + врахування конкретних інформаційних технологій, функцій підприємства та виробничого чи обчислювального середовища.

# **3.5. Програмна реалізація захисту інформації ЦАТС**

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.

# **3.5.1. Безпека на фізичному рівні та серверному рівнях**

Комплекс заходів щодо забезпечення безпеки IP АТС починається саме з обмеження фізичного доступу до сервера. Ми розглянемо ті загрози, які виникають в цьому аспекті і способи їх усунення.

* + 1. Виведення сервера з ладу / викрадення.

Найпростіший тип атаки типу Відмова в Обслуговуванні (DoS, Denial of Service) - це фізичне вимикання сервера або руйнування апаратних частин.

Також в разі недотримання заходів строго доступу в серверну зловмисники можуть викрасти сервер або носії інформації - жорсткі диски, стрічки, компакт-диски та інші засоби, на яких може перебувати бекап конфігурації сервера або конфіденційна інформація (записи розмов). Для мінімізації даного роду ризиків необхідно розміщувати сервер в зоні обмеженого доступу і виробити регламент входу / виходу обслуговуючого персоналу.

Додатковим заходом може бути кріплення сервера до стійки тросом із замком.

2. Захист завантажувача.

Якщо сервер виявився в руках зловмисників на короткий інтервал часу, або в результаті викрадення, насамперед будуть зроблені спроби отримання доступу супер-користувача для внесення змін в системні файли і приховування слідів злому.

Одним з спосіб отримання пароля root є порушення нормальної процедури завантаження сервера шляхом редагування параметрів загрузчиков GRUB або LILO. Наприклад, якщо в параметрах завантаження ядра передати init = / bin / bash, при завантаженні сервер не будуть виконуватися скрипти ініціалізації системи і породження процесів login. Замість цього відразу після завантаження ядра і модулів процес init передасть управління програмою bash, яка буде виконана з рутовкой привілеєм.

Щоб виключити дану ситуацію, слід використовувати спеціальні директиви загрузчиков, що забороняють зміни параметрів завантаження ядра, або вимагають авторизації доступу для їх проведення. Наприклад, для завантажувача lilo це опції password і restricted. Для grub це опція password

3. Консоль Asterisk

За замовчуванням, багато дистрибутиви Asterisk в момент завантаження сервера запускаються за допомогою скрипта safe\_asterisk, який відстежує працюють процеси і перезапускає Asterisk в разі випадкового падіння.

В скрипті safe\_asterisk є параметр TTY, який дорівнює 9 (TTY = 9). Дана опція при старті астеріска відкриває консоль під номером 9 (Alt + F9, або CTRL + ALT + F9 щоб в неї переключитися).

З огляду на можливість запуску з консолі команд ОС за допомогою знаку оклику, і враховуючи, що за замовчуванням Asterisk працює під обліковим записом суперкористувача, тільки володіючи доступом до 9-ї консолі можна легко скомпрометувати систему:

\* CLI>

\* CLI>! Bash

explorer ~ # whoami

root

explorer ~ #

Необхідно виключити заняття 9-й консолі шляхом коментування рядка з TTY = 9.

4. Обмеження для користувача акаунтів.

Так як Asterisk - вельми невибаглива до ресурсів сервера додаток (при середніх навантаженнях), то часто виникає спокуса використовувати сервер не тільки для телефонії, а й для інших потреб IT, таких як пошта, доступ в інтернет, корпоративний WEB, VPN, і тд. При цьому, доступ з сервера має не тільки адміністратор АТС, але і його колеги (адміністратори, програмісти).

Володіючи можливістю завантажувати і / або компілювати програми, такі користувачі потенційно можуть отримати повний доступ до системи в результаті уразливості ядра або інших компонентів ОС, і далі впровадити програму для приховування слідів присутності, і, таким чином, надовго зберегти несанкціоноване управління системою.

Щоб виключити таку можливість, слід закрити всі призначені для користувача екаунт в системі або прийняти ряд заходів щодо їх обмеження (використовувати оточення chroot, віртуальні сервера, спеціальний патчі типу GrSecurity, SELinux і ін.).

# **3.6. Обмеження привілеїв**

Більшість додатків не вимагає супер-привілеїв, в тому числі і Asterisk. Однак, за замовчуванням Asterisk працює під привілеєм root. Щоб це виправити, необхідно зробити наступне:

1. Налаштувати в asterisk.conf параметри runuser і rungroup (наприклад, додати групу asterisk і користувача asterisk, і запускати Asterisk під таким екаунт).

2. Зробити власником файлів / dev / zap / \* користувача Asterisk. Найпростіший спосіб - використовувати програму chown:

 chown \ -R asterisk.asterisk / dev / zap

Однак, сучасні дистрибутиви використовують динамічні системи прилади, такі як udev або devfs. Наприклад, в системі Gentoo Linux при установці Zaptel в папку /etc/udev/rules.d/ буде скопійований файл zaptel.rules, що має такий зміст:

 # Udev rules to generate the / dev / zap device files (if not yet provided

# By your distribution):

KERNEL == "zapctl", NAME = "zap / ctl"

KERNEL == "zaptranscode", NAME = "zap / transcode"

KERNEL == "zaptimer", NAME = "zap / timer"

KERNEL == "zapchannel", NAME = "zap / channel"

KERNEL == "zappseudo", NAME = "zap / pseudo"

KERNEL == "zap [0-9] \*", NAME = "zap /% n"

# Zaptel devices with ownership / permissions for running as non-root

SUBSYSTEM == "zaptel", OWNER = "asterisk", GROUP = "asterisk", MODE = "0660"

 }

Треба звернути увагу на те, яка обліковий запис використовується в опціях OWNER і GROUP, а також на режим MODE файлів. В результаті застосування зазначеного файлу при завантаженні модулів zaptel будуть створені такі пристрої:

 explorer ru # modprobe zaptel

explorer ru # ls \ -l / dev / zap /

total 0

crw-rw --- \ - 1 asterisk asterisk 196, 254 2008-10-21 3:35 channel

crw-rw --- \ - 1 asterisk asterisk 196, 0 2008-10-21 3:35 ctl

crw-rw --- \ - 1 asterisk asterisk 196, 255 2008-10-21 3:35 pseudo

crw-rw --- \ - 1 asterisk asterisk 196, 253 2008-10-21 3:35 timer

explorer ru #

4. Виправлення дозволів на папки. Так як при першій установці та запуску Asterisk з-під прівіленіі root були створені файли і папки, після зміни облікового запису роботи Asterisk доступу до цих файлів і папок вже немає. Щоб це виправити, треба запустити наступний скрипт:

 # \! / Bin / bash

chown \ - recursive asterisk: asterisk / var / lib / asterisk

chown \ - recursive asterisk: asterisk / var / log / asterisk

chown \ - recursive asterisk: asterisk / var / run / asterisk

chown \ - recursive asterisk: asterisk / var / spool / asterisk

chown \ - recursive asterisk: asterisk / usr / lib / asterisk

chown \ - recursive asterisk: asterisk / dev / zap

# ------------------------------------------------- - \ -

chmod \ - recursive u = rwX, g = rX, o = / var / lib / asterisk

chmod \ - recursive u = rwX, g = rX, o = / var / log / asterisk

chmod \ - recursive u = rwX, g = rX, o = / var / run / asterisk

chmod \ - recursive u = rwX, g = rX, o = / var / spool / asterisk

chmod \ - recursive u = rwX, g = rX, o = / usr / lib / asterisk

chmod \ - recursive u = rwX, g = rX, o = / dev / zap

# ------------------------------------------------- - \ -

chown \ - recursive root: asterisk / etc / asterisk

chmod \ - recursive u = rwX, g = rX, o = / etc / asterisk

# ------------------------------------------------- - \ -

# Asterisk needs to write to voicemail.conf for password change.

chmod g + w /etc/asterisk/voicemail.conf

chmod g + w, + t / etc / asterisk

# ------------------------------------------------- - \ -

# **3.7. Вимкнення сервісів**

Багато Linux/Unix дистрибутиви за замовчуванням запу скають багато непотрібні АТС сервіси, такі як служба друку, FTP, NFS і інші. Щоб побачити, які служби відкривають мережеві з'єднання, необхідно виконати команду netstat -atnup | grep LISTEN:

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State

PID / Program name

tcp 0 0 0.0.0.0:32768 0.0.0.0:\* LISTEN 3155 / rpc.statd

tcp 0 0 127.0.0.1:32769 0.0.0.0:\* LISTEN 3279 / xinetd

tcp 0 0 0.0.0.0:515 0.0.0.0:\* LISTEN 3279 / xinetd

tcp 0 0 0.0.0.0:199 0.0.0.0:\* LISTEN 3256 / snmpd

tcp 0 0 0.0.0.0:8008 0.0.0.0:\* LISTEN 4843 / httpd

tcp 0 0 0.0.0.0:139 0.0.0.0:\* LISTEN 3438 / smbd

tcp 0 0 0.0.0.0:111 0.0.0.0:\* LISTEN 3136 / portmap

tcp 0 0 0.0.0.0:6000 0.0.0.0:\* LISTEN 3516 / X

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 3265 / sshd

tcp 0 0 0.0.0.0:631 0.0.0.0:\* LISTEN 3907 / cupsd

tcp 0 0 127.0.0.1:25 0.0.0.0:\* LISTEN 3299 / sendmail: acce

tcp 0 0 0.0.0.0:443 0.0.0.0:\* LISTEN 4843 / httpd

За допомогою утліти Ntsysv потрібно вимкнути непотрібні нам служби.

# **3.8. Зміна SSH порту**

Служба SSH (Secure SHell), яка використовується для віддаленого входу на сервер – це вхід управління АТС. Використання наступних заходів

Зміна порту. Порт за замовчуванням SSH - 22-ий. Треба обрати інший порт, в діапазоні 1-65535.

Чітке вказання користувачів що мають доступ до системи в директиві [AllowUsers].

Заборонити прямий доступ користувача root. Це істотно ускладнить і швидше унеможливить атаку на перебір пароля, так як користувачу рут буде заборонен доступ в систему, навіть якщо буде введений його коректний пароль. Використовувати підсистему sudo для отримання Рутовського доступу при необхідності .

Використовуйте тимчасове обмеження по введенню пароля або сертифікати. Установка мінімально можливого часу для введення пароля, наприклад, 1 секунди, може добре збити з пантелику зловмисника.

Налаштування / etc / ssh / sshd\_config:

/ Etc / ssh / sshd\_config

AllowUsers amanzhula admin

Port 30222

Protocol 2

LoginGraceTime 1s

PermitRootLogin no

Зміна SIP порта

Порт за замовчуванням для обміну сигналами по протоколу SIP - 5060.

Для зміни порту варто зробити настройки /etc/asterisk/sip.conf

Port=5071

Централізоване логування

У разі успішної спроби захоплення сервер зловмисник може видалити сліди спроб злому для збереження непомітного контролю над сервером. Однак, в разі використання зовнішнього syslog сервер, це зробити не вдасться.

# **3.9. Безпечне налаштування Asterisk**

Контекст default

Контекст default взагалі не потрібно використовуати. Стандартні налаштування default :

exten => \_X., 1, Hangup

При такій настройці всі спроби дзвінків, які не пройшли нормальну авторизацію, будуть моментально завершуватися.

SIP-канал

Кожен тип каналу має як контексти по-замовчуванню, дзвінок потрапить в той контексе, який вказаний в опції context секції general sip.conf. Треба завжи для кожного клієнта створювати context які тільки призназначені йому. Наприклад:

[AquaService](law-codecs)

type = peer

host = 31.28.171.180

context = AquaService-Inbound

directmedia = no

insecure = port,invite

qualify = yes

callcounter = yes

# **3.10. Створення нових директорій для конфігурацій**

Створення нових директорій для конфігурацій за допомогою include вкладаємо директорії в стандартні конфігураційні директорії ext.conf та sip.conf окремо будуть директорії як для клієнта так і для провайдерів (див. рис. 3.3). Наприклад,

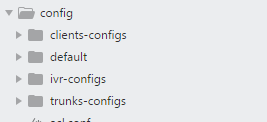


Рис. 3.3.Директорії конфігураці

На рис. 3.3 ще пристуні не тільки директорії клієнта, провайдера, а ще пристуні директорія системи попередньо записаних голосових повідомлень, що виконує функцію маршрутизації дзвінків та дефолтні конфігурації.

# **3.11. Поділ вхідних і вихідних дзвінків**

Варто чітко розділяти вхідні дзвінки та вихідні. що б було розуміння того що відбувається на станції. Коректні налаштування:

[Ibox-Inbound]

exten => \_X.,1,NoOp()

same => n,GoSub(HelperCIDFilter,s,1)

same => n,Set(CALLERID(name)=${EXTEN})

same => n,Verbose(0,!!! DEBUG !!! Ibox TEST CALL ${CALLERID(num)}-->${EXTEN})

same => n,Set(CDR(accountcode)=Ibox)

same => n,Goto(Alcatel-Outbound,57168,1)

[Ibox-Dialout]

exten => \_X.,1,NoOp()

same => n,GoSub(Ibox-Trunk,${EXTEN},1)

exten => \_X.,1,NoOp(Asterisk --> Ibox: ${CALLERID(num)})

same => n,GoSub(HelperMonitorStart,s,1)

same => n,GoSub(HelperCIDSet,s,1(6111))

same => n,Set(CDR(accountcode)=Ibox)

same => n,ChanIsAvail(SIP/Ibox-A&SIP/Ibox-B)

same => n,ExecIf($["${AVAILCHAN}" != " "]?Dial(${AVAILORIGCHAN}/${EXTEN}))

same => n,Return()

де Ibox-Inbound відповідає за маршрутизацію вхідних дзвінків. Кожен входить дзвінок запісиваеться до бази даних а так само записується розмова користувача. Після включення запису розмови дзвінок відправляється в фінальну інстанцію маршрутизацію на абонента.

Ibox-Dialout- відповідає за маршрутизації вихідних дзвінків, так само відбувається запис в базу даного дзвінка. включення запису розмови. привласнюється унікальний номер 6111 який ми передаємо провайдеру для ідентифікація. Так як у провайдера два сервера. ми використовуємо функцію яка перевіряє сервера провайдера в залежності який сервер працює на той і відправляємо дзвінок

# **3.12. Використання правил вихідної маршрутизації в ext.conf**

Слід чітко прописувати напрямки куди дзвонить клієнт. Тому що провайдер надає всі напрямки і у випадку злому. Зломщик може використовувати дане недопрацювання. Наприклад,

exten => \_3039.,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

exten => \_309[6-8].,1,Goto(National\_mobile\_Company EXTEN:1},1(${ARG1}))

exten => \_306[7,8].,1,Goto(National\_mobile\_Company ${EXTEN:1},1(${ARG1}))

exten => \_3050.,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

exten => \_3066.,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

exten => \_309[5,9].,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

exten => \_30[6,7,9]3.,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

exten => \_3091.,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

exten => \_3092.,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

exten => \_3094.,1,Goto(National\_mobile\_Company,${EXTEN:1},1(${ARG1}))

У даній ситуації ми працюємо з мобільними операторами України. Ми визначаємо куди дзвонить клієнт за кодом оператора. і відправляємо дзвінок у відповідність з кодом.

# **3.13. IAX2 аутентифікація**

Окремої згадки заслуговує алгоритм аутентифікації IAX2 з'єднань. При вхідному IAX2 дзвінку Asterisk виконується наступні послідовності перевірок.

Якщо присутнє поле username:

Шукає в файлі конфігурації iax.conf (і включених з нього файлів) секцію, ім'я якої збігається з username, в котрому type = user. Якщо збігів, не знайдено, відбудеться закриття каналу.

У знайденої секції перевіряється наявність параметрів allow / deny, і якщо IP адреса абонента збігається з deny, або не проходить ланцюжок allow, дзвінок завершується.

Перевіряється пароль. Якщо паролі не збігаються, дзвінок завершується.

Якщо у вхідному дзвінку вказано контекст призначення, Asterisk перевіряє наявність в налаштуваннях бенкету записи context = необхідний контекст.

Якщо контекст не вказано, дзвінок направляється на обробку в першу запис context =, в налаштуваннях транка .

Якщо в заголовку повідомлення нового дзвінка не міститься поле username, Asterisk виконує наступне:

Виконує пошук секції type = user, де немає поля secret, і немає атрибутів allow / deny. Якщо така секція знайдена, дзвінок приймається, і ім'ям username клієнта стає назва цієї секції.

Якщо збігів вище знайдено не було, Asterisk шукає секцію type = user, з зазначеним паролем secret або RSA ключем одночасно з allow / deny фільтром. Якщо така секція знайдена, і всі перевірки пройдені, Астеріск приймає дзвінок, і встановлює ім'ям username назву секції.

Виконує пошук секції type = user з встановленим паролем secret (або RSA ключем), але без фільтрів allow / deny. Якщо перевірка за паролем проходить, дзвінок приймається, і значення username встановлюється назвою секції.

Asterisk відкидає дзвінок.

Які можливі несподівані наслідки має така схема аутентифікації? Можна застосовувати атаку типу brute force (грубої сили), перебираючи паролі пользоваталей, навіть не знаючи їх username! При достатній кількості записів бенкетів в iax.conf, ймовірність подброра пароля до однієї з них досить висока. Як знизити ризики такої атаки?

Включити сповільнену реакцію (delayreject = yes в [general] налаштуваннях iax.conf). Це дозволить уповільнити посилку негативної відповіді сервера. знижуючи швидкість перебору по словнику. Однак, зловмисник може припустити про наявність даної опції, і перебудувати атаку, не чекаючи відповіді, вважаючи, що позитивну відповідь прийде швидко.

Використовувати атрибути-фільтри allow / deny.

Створити спеціальний гостьовий аккаунт без пароля і мережевих обмежень. Таким чином, алгоритм аутентіфікаіі "спрацює" до перевірки пароля, і атака по словнику вже не має сенсу, так як приймається дзвінок з будь-яким паролем. Ось так виглядає гостьовий екаунт:

iax.conf

 [Guest]

type = user

context = guest

extensions.conf

 [Guest]

exten => \_X., 1, Hangup

exten => i, 1, Hangup

Однак, відкриття гостьового входу загрожує іншими наслідками - атаками по типу відмови в обслуговуванні. Тому найбільш сильною захистом IAX2 клієнтів буде використання аутентифікації по RSA ключів, так як підібрати такий ключ практично неможливо.

Прив'язка користувача до IP адресою.

Найчастіше SIP користувачі знаходяться в локальній мережі з постійними IP адресами, або централізовано керованими за допомогою DHCP. В якості додаткової міри безпеки можна явно вказувати адресу для підключення конкретного бенкету, наприклад,

[amanzhula]

type = friend

host = dynamic

username=amanzhula

secret=amanzhula

insecure = port,invite

qualify = yes

callcounter = yes

context = amanzhula

host = 192.168.7.10

Також можна підвищити захищеність шляхом завдання явно дозволених або забороненних хостів або мереж за допомогою директив permit / deny, як показано в прикладі нижче:

[amanzhula]

type = friend

host = dynamic

username=amanzhula

secret=amanzhula

insecure = port,invite

qualify = yes

callcounter = yes

context = amanzhula

permit = 195.242.0.0 / 255.255.0.0

У даній настройці дозволяється встановлювати лише з мережі 195.242.0.0/16.

[amanzhula]

type = friend

host = dynamic

username=amanzhula

secret=amanzhula

insecure = port,invite

qualify = yes

callcounter = yes

context = amanzhula

deny = 195.242.0.0 / 255.255.0.0

У даній настройці забороняється встановлювати з’єднання з мережі 195.242.0.0/16.

# **3.14. Одночасне кількість розмов**

Коли з якої-небудь причини SIP акаунт клієнта користувача скомпрометований. Наприклад, в результаті підключення з публічного комп'ютера готелю або інтернет-кафе користувач забув видалити конфігурацію софтфона, і SIP username / password потрапив в руки зловмисника, який продає отриману обліковий запис SIP бенкету на

"Чорному ринку" VOIP трафіку. В цьому випадку, якщо не обмежити в Астеріск кількість максимально можливих одночасних розмов на користувача, через АТС може пройти велику кількість дзвінків, до тих пір, поки це не помітять. Але навіть після блокування скомпрометованої облікового запису рахунок за переговори пред'явити буде нікому.

У переважній більшості випадків користувачі роблять один вихідний дзвінок. Виняток становить запрошення в конференцію. У будь-якому випадку, адміністратору слід встановити ліміт в 1 одночасний дзвінок за замовчуванням для всіх, явно збільшуючи ліміт там де це необхідно. Ліміт на одночасні дзвінки встановлюється за допомогою функції GROUP, а перевіряється за допомогою GROUP\_COUNT.

[proverka]

exten => \_X.,1,Gosub(сall-limit,${EXTEN},1)

same => \_X.,n,Dial(SIP/${EXTEN}@provider)

[сall-limit]

exten => \_X.,1,Set(GROUP()=${EXTEN})

same => \_X.,n,GotoIf($[ ${GROUP\_COUNT()} > 5 ]?busy)

same => \_X.,n,Return

same => n(busy),hangup(17)

Дана програма виконує перевірку на кількість одночасних викликів.

За допомогою змінної $ {GROUP\_COUNT () ми задаємо кількість одночасних викликів, якщо кількість одночасних викликів більше 5 вона завершуємо дзвінок зі статусом зайнято, якщо кількість одночасних викликів менше 5 то дзвінок успішно відбувається

# **3.15 Захист Asterisk за допомогою iptables**

Iptables - утиліта командного рядка, є стандартним інтерфейсом управління роботою брандмауера (брандмауера) Netfilter для ядер Linux/Unix починаючи з версії 2.4. З її допомогою створюють і змінюють правила, що керують фільтрацією і перенаправленням пакетів.

Перевіримо чи встановлено IPTables

[Root@kv-NAU] # rpm -q iptables

iptables-1.3.5-5.3.el5\_4.1

Подивимося поточні правила які встановлені

[root@ kv-NAU ]# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT icmp -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Ця команда дозволить всі вхідні підключення що дозволить уникнути блокування з'єднання, якщо конфігурація проводиться через ssh.

# Iptables –F

Дана команда скине всі поточні правила за замовчуванням і застосує тільки створене нами правило яке ми створили.

Це правило дозволяє все підключення на адаптер loopback. Інтерфейс loopback визначається системою як lo і за замовчуванням має адресу 127.0.0.1 Команда -А додає нове правило в кінець заданої ланцюжка INPUT. Опція -i разом ім'ям інтерфейсу lo дозволяє всі види трафіку через заданий інтерфейс. Опція -j вказує на мету даного правила ACCEPT, вжити всіх підключення.

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Далі присутня опція -m яка використовується для завантаження модуля state. Модуль state перевіряє стан пакета і визначає чи є він новим-NEW, вже створеним-ESTABLISHED або новим, але пов'язаним-RELATED з уже встановленим з'єднанням. Стан ESTABLISHED вказує на те, що пакет належить вже встановленому з'єднанню через яке пакети йдуть в обох напрямках. Ознака NEW увазі, що пакет відкриває нове з'єднання або пакет належить односпрямованому потоку. Ознака RELATED вказує на те що пакет належить вже існуючому з'єднанню, але при цьому він відкриває нове з'єднання.

Це правило додається до ланцюжку INPUT і каже, що все пакети, що приходять по протоколу TCP (-p tcp), на порт 22 (-dport 22), повинні бути прийняті (-j ACCEPT). Використовується для підключення по ssh c портом за замовчуванням.

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Ці правила дозволяють ініціацію підключеня до сервера Asterisk від віддалених користувачів або провайдера.

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p udp -m udp --dport 5060 -j ACCEPT

iptables -A INPUT -p udp -m udp --dport 5061 -j ACCEPT

iptables -A INPUT -p udp -m udp --dport 10000:20000 -j ACCEPT

iptables -A INPUT -p udp -m udp --dport 4569 -j ACCEPT

iptables -A INPUT -p tcp -m tcp --dport 5038 -j ACCEPT

Дане правило дозволяє тільки підключення з певних ip адрес і мереж

iptables -A INPUT -p udp -m udp -s 123.123.123.123 --dport 5060 -j ACCEPT

iptables -A INPUT -p udp -m udp -s 192.168.0.0/24 --dport 5060 -j ACCEPT

# **3.16 Модуль підвищення захисту АТС**

Модуль починається з измения стандартних файлів конфігурації автоматичної телефонної станції нижче надано назва стандартних файлів конфігурації для АТС (рис. 3.4).

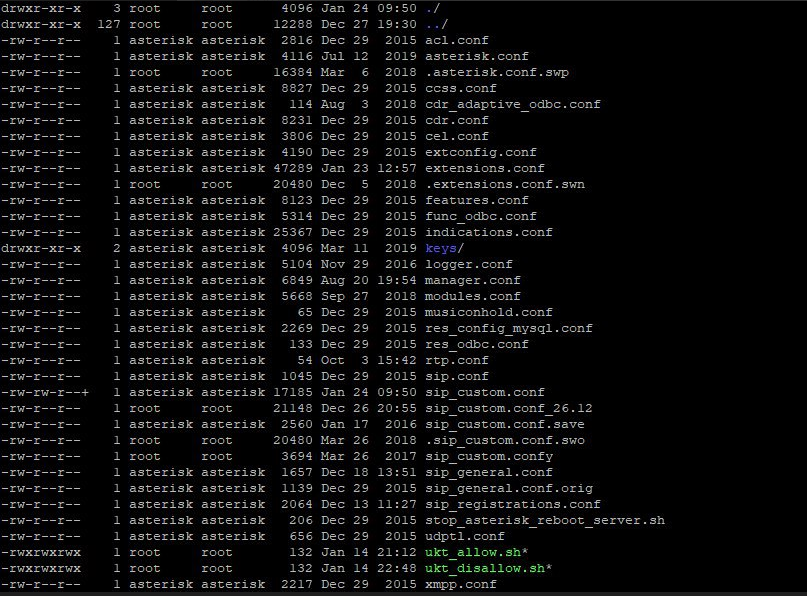


Рис. 3.4. Стандартні файли конфігурації для АТС

Варто чітко разгронічіть всі налаштування маршрутизації клієнтів, провайдерів. в різні файли. Так само не варто забувати про різні функції у вигляді голосового Дерева. Тому створюємо файли :

Clients-config

Trunk-config

Ivr-Conf

як показано на рис. 3.5.

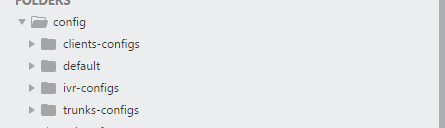


Рис. 3.5. Створені файли

Дані файли ми за допомогою INCLUDE вкладаємо в стандартні конфіги (рис. 3.6).

Закриваємо їх на редагування і шифруємо стандартні файли конфігурації (рис. 3.7).

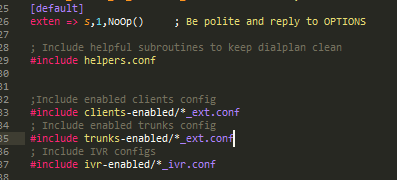


Рис. 3.6. Вкладення файлів через include

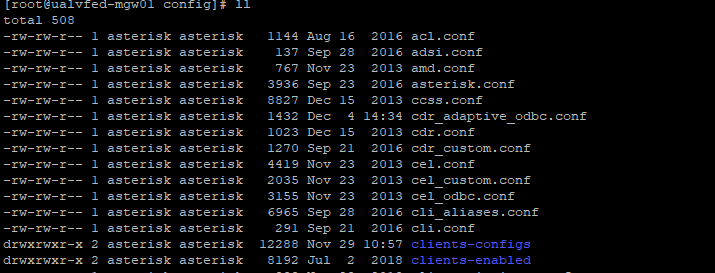




Рис. 3.7. Конфігураційні файли астериск

Щоб додати нове підключення коштує створити папку з даними підключенням і додати туди клієнта варто прописати конфігурації (рис. 3.8).



Рис. 3.8. Нове підключеня

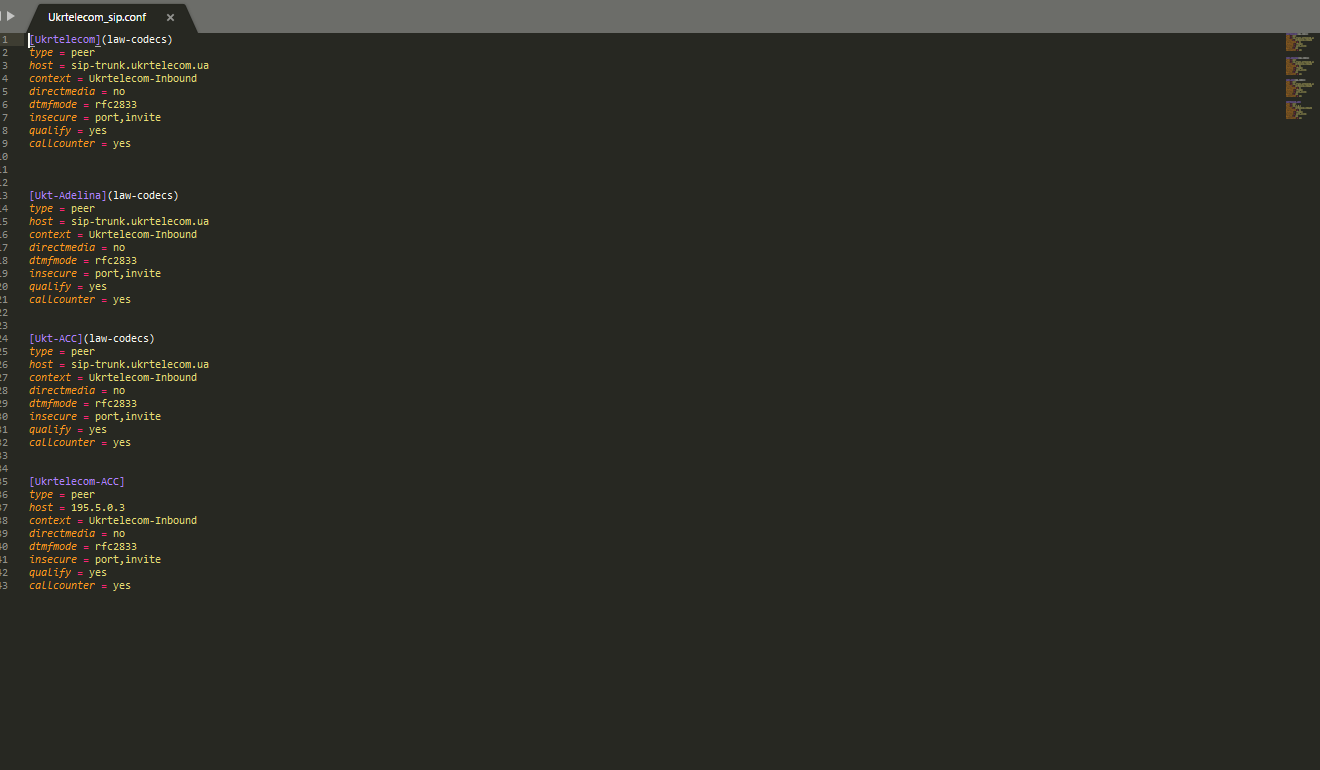


Рис. 3.9. Конфігурація підключення

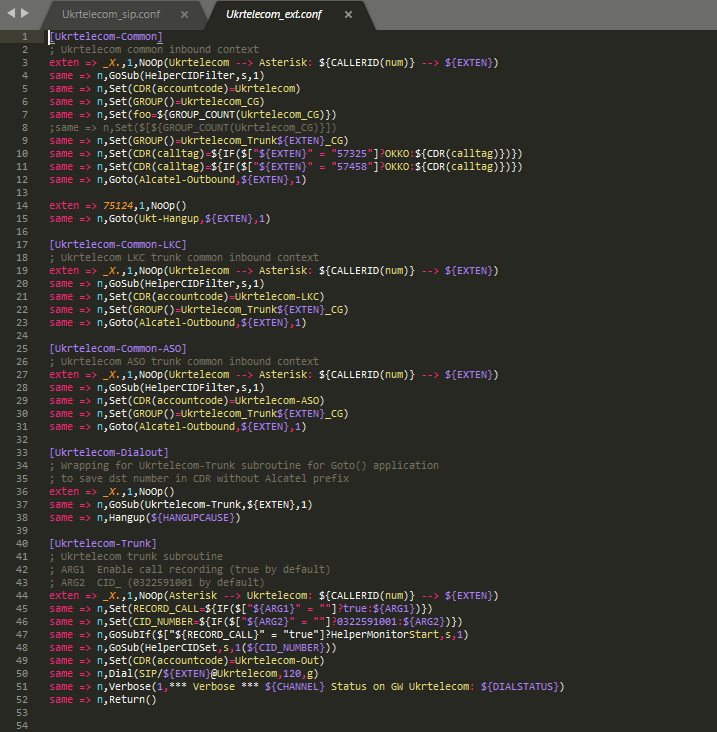


Рис. 3.10. Конфігурація підключення

Що б конфігурація вступила в силу потрібно в стандартному методі перезавантажити конфігурації. Ми перезавантажили конфігурації але нічого не відбулося (рис. 3.11).

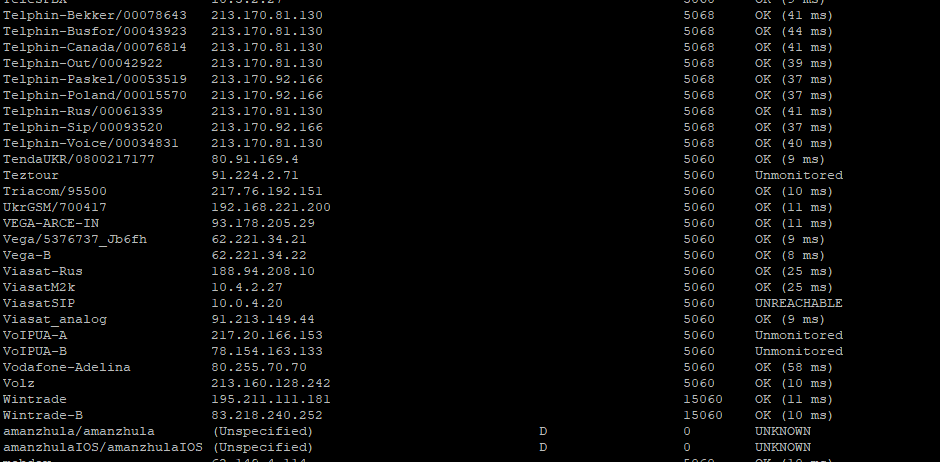


Рис. 3.11. Перезавантаження конфігурації

Що б конфігурація вступила в силу варто з консолі запустити програму astenable cliet Ukrtelecom. Ми бачимо що відпрацювала програма (рис. 3.12).

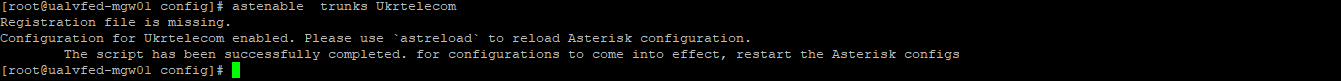
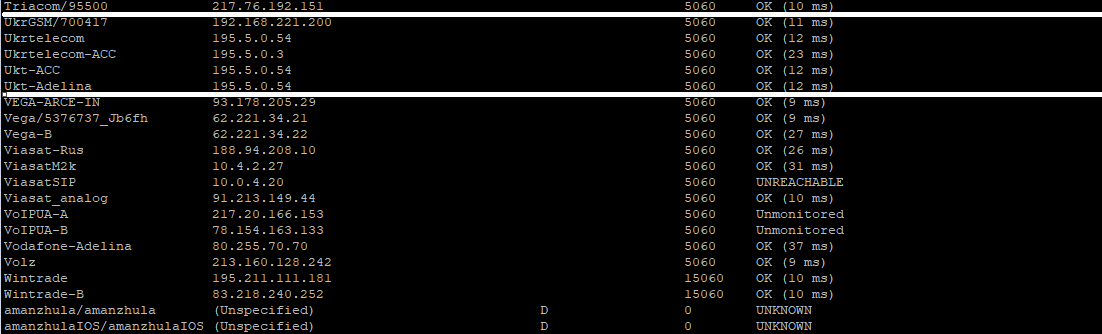


Рис. 3.12. результати роботи astenable cliet Ukrtelecom

Перезавантажуємо конфігурацію і бачимо чітко що даний клієнт з'явився.



Даний метод полягає що закрити всі конфігураційні файли, розбити кожне підключення на клієнт провайдер. і за допомогою програми ми довантажувати даний кожне нове підключення в стандартний конфігураційний файл.

#### **3.17. Висновок**

Архітектура мережі IP-телефонії являє собою з'єднані по IP-мережі Шлюзи в телефонну мережу, які надають безпосередній інтерфейс абонентові і здійснюють кодування, стиснення і пакетізацию голосу / факсу та їх відновлення. Весь механізм взаємодії шлюзів і облік проводиться диспетчерами. Для зручності видаленої конфігурації і адміністрування мережі може бути використаний Монітор. Ці три компоненти у різних виробників можуть називатися по-різному, але всі вони виконують функції, узагальнені вище. Крім описаних вище вимог, устаткування для IP-телефонії може підтримувати ще деякі можливості.

# **ВИСНОВКИ**

Забезпечення безпеки мережі вимагає постійної роботи і пильної уваги до деталей.

У даному розділі було розглянуто основні типи несанкціонованого доступу на фізичному рівні та серверному рівні та також вирішення, а саме:

Виведення сервера з ладу / викрадення :

Захист завантажувача :

Консоль Asterisk

БЕЗПЕКА НА СЕРВЕРНОМУ РІВНІ

Обмеження для користувача акаунтів

Обмеження привілеїв

Безпечне налаштування Asterisk

Створення нових директорій для конфігурацій

Поділ вхідних і вихідних дзвінків

Комбінуванням засобів захисту можна домогтися хорошою захищеності інформації. Неможливо абсолютно захистити інформацію від несанкціонованого доступу Функціонування механізму захисту повинен плануватися і забезпечуватися поряд з плануванням і забезпеченням основних процесів АТС.

Долслідження проводилось в ARCE contact center

ARCE contact center - надійний Аутсорсінговий партнер провідних українських і міжнародних компаній. На сьогоднішній день в ARCE Сontact сenter працює більше 1000 співробітників, які обслуговують клієнтів з усього світу на більш ніж десяти мов світу

### **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Глобальное исследование утечек корпоративной информации и конфиденциальных даннях, 2011. Аналитический центр InfoWatch – Москва, 2013. – 30 с.
2. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – К.: ДСТС31 СБ

України, 1999. – 26 с.

1. Звіт по проекту «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ. Частина 2. Основні технічні рішення», – Національна Академія Наук України, Інститут Програмних Систем – Київ, 2004. – 77 с.
2. Антонюк А.А., Жора В.В. Моделювання доступу та каналів витоку в інформаційних системах // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – № 3. – С. 156–160.
3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – НиТ, Санкт–Петербург, 2004. – 384 с.
4. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99.–К.. ДСТСЗІ СБ України, 1999. – 16 с.
5. Закон України 3855–ХІІ від 21.01.1994 «Про державну таємницю» // Голос України – 1994. – 29 с.
6. Вікіпедія (Електронний ресурс) / Спосіб доступу: URL: http://uk.wikipedia.org. – Заголовок з екрана.
7. Указ Президента України № N 505/98 від 22.05.1998 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» // Урядовий кур’єр від 09.07.1998
8. Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України (Електронний ресурс) / Спосіб доступу: URL:

http://www.dstszi.gov.ua/dstszi/control/

uk/publish/article;jsessionid=140F77BFF5167554CD3353B12F059064?art\_id =78319&cat\_id=39181 – Заголовок з екрана.

1. Институт компьютерных технологий / Защита информации в ПЭВМ

(Електронний ресурс) / Спосіб доступу: URL: http://www.ict.com.ua/ ?lng=1&sec=8&art=41 – Заголовок з екрана.

1. Система захисту інформації ЛОЗА (Електронний ресурс) / Спосіб доступу: URL: http://avtoprom.kiev.ua/product2.html – Заголовок з екрана.
2. АНКАД – Средства защиты информации, защита государственной тайны, защита персональних даннях, шифрование (Електронний ресурс) / Спосіб доступу: URL: http://www.ancud.ru/srd.html – Заголовок з екрана.
3. Products & Services – Cisco Systems (Електронний ресурс) / Спосіб доступу: URL: http://www.cisco.com/en/US/products/index.html – Заголовок з екрана.
4. Secret Net система защиты информации от несанкционированного доступа (Електронний ресурс) / Спосіб доступу: URL: http://www.securitycode.ru/ products/secret\_net – Заголовок з екрана.
5. Предотвращение утечек данных (Електронний ресурс) / Спосіб доступу: URL: http://www.sovit.net/articles/technologies/data\_loss\_prevention/ –

Заголовок з екрана.

1. Защита от утечек даннях – DLP–решения (Електронний ресурс) / Спосіб доступу: URL: http://www.protectme.ru/infosec/dlp – Заголовок з екрана.
2. Статья DLP – DataLoss / LeakPrevention – Технологии предотвращения утечек конфиденциальной информации– TADVISER (Електронний ресурс) / Спосіб доступу: URL: http://www.tadviser.ru/index.php/Статья:DLP – Заголовок з екрана.
3. Ефременко Наталья. Онтологии в DLP – системах третьего поколения. – Information Security, №4. – 2009.
4. Векторная модель текста (Електронний ресурс) / Спосіб доступу: URL: http://www.neural.ru›dictionary/Векторная модель текста – Заголовок з екрана.
5. Никоненко А.А. Обзор баз знаний онтологического типа (Електронний ресурс) / Спосіб доступу: URL: http://lingvoworks.org.ua/index.php?option= com\_content&view=article&id=57:2009–12–09–11–34– 5&catid=2:misc&Itemid=3 – Заголовок з екрана.
6. В.Б. Задоров. До переосмислення деяких загальносистемних понять з метою інтеграції онтологій та комп’ютерних інформаційних систем, – Стаття, Київський національний університет будівництва і архітектури, – 2010 р.
7. Технологии применения онтологий | Онтологический инжиниринг и управление знаниями | Теория (Електронний ресурс) / Спосіб доступу: URL: http://bigc.ru/theory/km/onto\_technologies.php – Заголовок з екрана.
8. Болотова В.А. Григорьев А.В. Инструментальные средства создания баз знаний на основе системы онтологій (Електронний ресурс) / Спосіб доступу: URL: http://www.masters.donntu.edu.ua/2010/fknt/bolotova/library/tez1.htm –

Заголовок з екрана.

1. Рейтинг зарплат 2011 року (Електронний ресурс) / Спосіб доступу: URL: http://rada.kosiv.info/kosivs/tidings/8742–rеiting–zаrplаt–2011–rокu.html –

Заголовок з екрана.

1. Microsoft Україна: програми, технології, онлайн, комп'ютери, ігри

(Електронний ресурс) / Спосіб доступу: URL: http://www.microsoft.com/uk–ua/default.aspx – Заголовок з екрана.

# Додаток А .Захист конфігурацій за допомогою програмного модулю

Дана програма включає зміни які вироблені в файлах конфігураціях. Оновлює або додає файли конфігурацій в яких були проведені зміни в певні директорії

function usage {

echo "Usage: astenable {client|trunk|ivr} <target\_name>"

echo "Examples:";

echo " \* To enable configuration for Volition\_sip.conf and Volition\_ext.conf files, run:";

echo " astenable client Volition";

echo " \* To enable private/local configuration for private\_SKM\_sip.conf and private\_SKM\_ext.conf , run:";

echo " astenable trunk SKM";

exit 1;

}

if [ $# -lt 2 ]; then usage; fi;

case $1 in

tr\* ) target=trunks;;

cl\* ) target=clients;;

ivr ) target=ivr;;

\* ) echo "Error: Invalid target '$1' specified."; usage

esac

target\_name=$2

configs\_dir=/etc/asterisk/${target}-configs

enabled\_dir=/etc/asterisk/${target}-enabled

if [ ! -d ${enabled\_dir} ]; then

echo "Error: Target directory ${enabled\_dir} does not exists.";

exit 255;

fi

# Check format of sip.conf file (dos or unix)

grep -c $'\r\n$' /etc/asterisk/sip.conf &>/dev/null

if [ $? -eq 0 ]; then

NL="\r\n"

else

NL="\r"

fi

# breakpoint

#exit 0;

function conf\_unavail {

echo "Error: Configuration file is missing.";

echo "Please check if file $1 exists.";

exit 2;

}

if [ ${target} = "trunks" -o ${target} = "clients" ]

then

if [ ! -e ${configs\_dir}/${target\_name}\_sip.conf ]; then

if [ ! -e ${configs\_dir}/private\_${target\_name}\_sip.conf ]; then

conf\_unavail ${configs\_dir}/${target\_name}\_sip.conf;

else

conf\_sip=private\_${target\_name}\_sip.conf

fi

else

conf\_sip=${target\_name}\_sip.conf

fi

if [ ! -e ${configs\_dir}/${target\_name}\_ext.conf ]; then

if [ ! -e ${configs\_dir}/private\_${target\_name}\_ext.conf ]; then

conf\_unavail ${configs\_dir}/${target\_name}\_ext.conf;

else

conf\_ext=private\_${target\_name}\_ext.conf

fi

else

conf\_ext=${target\_name}\_ext.conf

fi

if [ ! -e ${configs\_dir}/${target\_name}\_reg.conf ]; then

if [ ! -e ${configs\_dir}/private\_${target\_name}\_reg.conf ]; then

echo "Registration file is missing.";

#conf\_unavail ${configs\_dir}/${target\_name}\_reg.conf;

else

conf\_reg=private\_${target\_name}\_reg.conf

fi

else

conf\_reg=${target\_name}\_reg.conf

fi

test -e ${enabled\_dir}/${conf\_sip} || ln -s ${configs\_dir}/${conf\_sip} ${enabled\_dir}

test -e ${enabled\_dir}/${conf\_ext} || ln -s ${configs\_dir}/${conf\_ext} ${enabled\_dir}

test -e ${enabled\_dir}/${conf\_reg} || ln -s ${configs\_dir}/${conf\_reg} ${enabled\_dir}

if [ $? -eq 0 ]; then

echo "Configuration for ${target\_name} enabled. Please use \`astreload\` to reload Asterisk configuration."

exit 0

else

echo "Error: Configuration for ${target\_name} is not enabled. Please see error message above."

exit 1

fi

fi

if [ ${target} = "ivr" ]

then

if [ ! -f ${configs\_dir}/${target\_name}\_ivr.conf ]; then

echo "Error: Some of the configuration files are missing.";

echo "Please check if file ${target\_name}\_ivr.conf exists in ${configs\_dir}";

exit 2;

fi

test -f ${enabled\_dir}/${target\_name}\_ivr.conf || ln -s ${configs\_dir}/${target\_name}\_ivr.conf ${enabled\_dir}

if [ $? -eq 0 ]; then

echo "Configuration for ${target\_name} enabled. Please use \`astreload\` to reload Asterisk configuration."

exit 0

else

echo "Error: Configuration for ${target\_name} is not enabled. Please see error message above."

exit 1

fi

fi