Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Лісничого Владислава Олександровича*

академічної групи *125м-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи підвищення інформаційної безпеки інтерактивної голосової служби (IVR)*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.ф.-м.н., проф. Гусєв О.Ю.			
розділів:				
спеціальний	ас. Мацюк С.М.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Лісничому В.О.* **академічної групи** *125м-17-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи підвищення інформаційної безпеки інтерактивної голосової служби (IVR)*

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.2018 № 2025-л_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *інтерактивне голосове меню (IVR-система)*

Предмет досліджень *методи підвищення інформаційної безпеки інтерактивної голосової служби*

Мета *дослідити ефективність засобів забезпечення інформаційної безпеки інтерактивної голосової служби*

Вихідні дані для проведення роботи *законодавство України та міжнародні стандарти у сфері кібербезпеки, існуючі алгоритми оцінки загроз інформаційної безпеки підприємства, статистичні дані з інцидентів інформаційної безпеки при використання IP-телефонії*

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна *полягає у вирішенні проблеми комплексного захисту інформаційних ресурсів ІТС приватного підприємства від спектру мережевих атак, спрямованих на отримання несанкціонованого доступу до інформації*

яка оброблюється засобами IVR CRM-системи

Практична цінність *розробка рекомендацій щодо реалізації комплексу засобів захисту IVR-системи*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

наведені рекомендації повинні бути враховані щодо використання платіжних карток VISA і MasterCard при замовлені послуг за допомогою IVR-системи

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *від впровадження на підприємстві захищеної IVR-системи, очікується позитивна динаміка розвитку підприємства, за рахунок зниження витрат на систему захисту інформації*

Соціальний ефект *полягає у швидкому розслідувані інцидентів кібербезпеки, що зменшить час на відновлення роботи IVR-системи після можливої мережевої атаки*

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ Гусєв О.Ю.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Лісничий В.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., 4 додатки, 25 джерел.

Об’єкт розробки: інтерактивне голосове меню.

Мета дипломної роботи: дослідити ефективність засобів забезпечення інформаційної безпеки інтерактивної голосової служби.

У першому розділі визначена актуальність роботи, наведені особливості роботи та архітектура контакт-центрів, визначені переваги використання IP-телефонії, розглянуті основні функції інтерактивної голосової служби (IVR-системи).

У другому розділі наведена архітектура об’єкта досліджень, розглянуті основні загрози направлені на порушенні роботи інтерактивної голосової служби, розроблена модель порушника, обрано функціональний профіль захищеності, дані рекомендації щодо реалізації комплексу засобів захисту, побудована матриця розмежування доступу до IVR-системи, наведені рекомендації щодо використання платіжних карток VISA і MasterCard при замовлені послуг за допомогою IVR-системи.

Запропоновані методи підвищення інформаційної безпеки можуть використовуватися не лише для конкретної IVR–системи, що була розглянута в дипломній роботі, а й для інших систем, які були розроблені і обслуговуються компанією-власником. Приведені методи допоможуть підвищити рівень інформаційної безпеки не тільки компаніям, що тільки починають використовувати інтерактивні голосові служби але й компаніям, що вже давно використовують дане бізнес рішення.

IVR, АНАЛІЗ ЗАГРОЗ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, МЕТОДИ ЗАХИСТУ, ПРОФІЛЬ ЗАХИЩЕНОСТІ, ІНТЕРАКТИВНА ГОЛОСОВА СЛУЖБА.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., 4 приложений, 25 источников.

Объект разработки: интерактивное голосовое меню.

Цель дипломной работы: исследовать эффективность средств обеспечения информационной безопасности интерактивной голосовой службы.

В первом разделе определена актуальность работы, приведены особенности работы и архитектура контакт-центров, определены преимущества использования IP-телефонии, рассмотрены основные функции интерактивной голосовой службы (IVR-системы).

Во втором разделе приведена архитектура объекта исследований, рассмотрены основные угрозы направлены на нарушении работы интерактивного голосового службы, разработана модель нарушителя, выбран функциональный профиль защищенности, даны рекомендации по реализации комплекса средств защиты, построенная матрица разграничения доступа к IVR-системы, приведены рекомендации по использования платежных карт VISA и MasterCard при заказе услуг с помощью IVR-системы.

Предложенные методы повышения информационной безопасности могут использоваться не только для конкретной IVR-системы, которая была рассмотрена в дипломной работе, но и для других систем, которые были разработаны и обслуживаются компанией-владельцем. Приведенные методы помогут повысить уровень информационной безопасности не только компаниям, которые только начинают использовать интерактивные голосовые службы, но и компаниям, которые уже давно используют данное бизнес решения.

IVR, АНАЛИЗ УГРОЗ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, СПОСОБЫ ЗАЩИТЫ, ПРОФИЛЬ ЗАЩИЩЕННОСТИ, ИНТЕРАКТИВНОЕ ГОЛОСОВОЕ СЛУЖБА.

ABSTRACT

Explanatory note: ___ p., __ fig., __ tab., 4 application, 25 sources.

Object of development: interactive voice menu.

The purpose of the thesis: to investigate the effectiveness of information security tools interactive voice service.

In the first section, the relevance of the work is determined, the features of the work and the architecture of contact centers are given, the advantages of using IP telephony are defined, and the main functions of the interactive voice service (IVR system) are considered.

The second section shows the architecture of the object of research, discusses the main threats aimed at disrupting the work of the interactive voice service, developed an intruder model, selected a functional security profile, made recommendations on the implementation of a set of protection tools, constructed an access differentiation matrix for the IVR system, VISA and MasterCard cards when ordering services using an IVR system.

The proposed methods of enhancing information security can be used not only for a specific IVR system, which was considered in the thesis, but also for other systems that were developed and maintained by the company-owner. These methods will help improve the level of information security not only for companies that are just beginning to use interactive voice services, but also for companies that have been using this business solution for a long time.

IVR, ANALYSIS OF THREATS, UNAUTHORIZED ACCESS, PROTECTION METHODS, SECURITY PROFILE, INTERACTIVE VOICE SERVICE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

CRM	–	Customer Relationship Management System;
ICMP	–	Internet Control Message Protocol;
IP	–	Internet Protocol;
ISP	–	Internet Service Provider;
IVR	–	Interactive Voice Response;
SSL	–	Secure Sockets Layer;
TCP	–	Transmission Control Protocol;
VMM	–	Virtual Memory Management;
VPN	–	Virtual Private Network;
АС	–	автоматизована система;
БД	–	база даних;
ІС	–	інформаційна система;
ІТС	–	інформаційно-телекомунікаційна система;
КЗЗ	–	комплекс засобів захисту;
КМ	–	комп’ютерна мережа;
ЛОМ	–	локальна обчислювальна мережа;
НД	–	нормативний документ;
НСД	–	несанкціонований доступ;
ОС	–	операційна система;
СЗІ	–	система захисту інформації;
СКБД	–	система керування базами даних;
ТЗІ	–	технічний захист інформації.

ЗМІСТ

с.

ВСТУП

Інтерактивні голосові сервіси набувають широкого поширення в сфері телефонного обслуговування, це обумовлено доступністю обладнання комп'ютерної телефонії третього покоління та необхідністю швидко та якісно надавати інформацію, проводити сповіщення великої кількості клієнтів, правильно розподіляти потік вхідних викликів, що надходять до Call/контакт-центрів. Але однією з первинних причин, що спонукає компанії прийняти рішення щодо впровадження і використання інтерактивних голосових систем є зменшення витрат завдяки скороченню персоналу обслуговуючого телефонні звернення клієнтів. Проте, дуже часто, заощаджування коштів включає в себе не лише встановлення IVR – системи (Interactive Voice Response), алей відмову від забезпечення належного рівня інформаційної безпеки в самій системі, тобто компанії не вважають за необхідне витрачати кошти на забезпечення конфіденційності, цілісності і доступності як клієнтської так і власної інформації. Таке відношення може призвести до розкрадання баз даних компанії, порушенню коректної роботи системи голосового меню або, взагалі, до знищення цього інформаційного ресурсу.

Приймаючи рішення щодо впровадження IVR – системи, компанії або звертаються до постачальників даних послуг, які в свою чергу встановлюють власні програмно-технічні засоби, або ж будують систему самостійно використовуючи власне обладнання та існуючі програмні засоби.

В першому варіанті, компанія-постачальник пропонує, відповідно до вимог компанії-замовника, конкретне програмно-технічне рішення, зазвичай це є готовий IVR сервер, що має певні технічні характеристики, на якому встановлене конкретне програмне забезпечення, що розроблене компанією – постачальником. Компанія замовник може змінювати лише загальні налаштування системи, структуру голосового меню, схему переадресацій, умови звітності та інші необхідні для роботи параметри. Більш глибокі налаштування і обслуговування системи здійснює компанія-постачальник.

Такий підхід до впровадження і використання IVR – систем вимагає великих грошових інвестицій, порівняно з тим випадком, коли компанія сама будує і обслуговує IVR – систему, але він є ефективним у випадках, коли необхідна негайна побудова системи, або компанія-замовник вважає за краще використовувати даний сервіс для власного бізнесу, не вдаючись у подробиці, передаючи технічні та програмні проблеми сторонній компанії.

Другий варіант побудови IVR – систем є більш дешевшим за перший, але повне налаштування системи повинна здійснювати компанія – власник.

З точки зору інформаційної безпеки, другий варіант є більш сприятливим, тому що компанія повністю керує процесом розробки, впровадження і використання IVR – системи, тим самим зменшуючи доступ сторонніх осіб до інформації що циркулює в інтерактивній голосовій службі. Також, самостійне створення і обслуговування IVR – системи, дозволяє на власний розсуд встановити необхідний рівень інформаційної безпеки, повністю контролюючи процес захисту даного бізнес-рішення.

Метою дипломної роботи є забезпечення інформаційної безпеки інтерактивної голосової служби та надання загальних рекомендацій щодо захисту інформації в IVR – системах, коли компанія повністю керує процесом створення і обслуговування даного інформаційного ресурсу.

Все більше запитів, що надходять в Call/контакт – центри оброблюється в автоматичному режимі, навіть питання, для вирішення яких необхідна конфіденційна інформація клієнта. Тому забезпечення інформаційної безпеки IVR – систем є важливою задачею компанії, що їх використовують.

РОЗДІЛ 1. АНАЛІЗ ПРОЦЕСІВ ВЗАЄМОДІЇ СИСТЕМИ IVR В ІТС ПІДРИЄМСТВА

1.1 Актуальність проблематики

В наш час кожна людина бажає мати зв'язок і отримувати інформацію миттєво, де завгодно і в самих різних формах: аудіо, дані, відео, мультимедіа. Всі ці послуги вимагають дуже високих технологій, серед яких на початку XXI століття гідне місце зайняли Call-центри й обладнання комп'ютерної телефонії третього покоління.

На світовому телекомунікаційному ринку яскраво проявилося те, що темпи зростання доходів, одержуваних від надання додаткових інфокомунікаційних послуг суттєво перевищують темпи зростання доходів від традиційних послуг – власне забезпечення комутованих з'єднань. Безсумнівно, що сучасний оператор-постачальник послуг не тільки повинен бути здатний запропонувати широкий спектр спеціалізованих послуг, орієнтованих на задоволення потреб окремих груп користувачів, а й уміти швидко і за розумних витратах впроваджувати нові види послуг.

Комп'ютери вже вміють приймати і сортувати телефонні виклики, виконувати сповіщення абонентів, надавати абонентам доступ до баз даних, видавати інформацію про розклад поїздів або літаків, про наявність квитків або товарів на складах і в магазинах і т.п. Крім того, комп'ютерна телефонія - це сервісні телефонні картки, інтегрований корпоративний офіс, запис телефонних переговорів і багато іншого.

Програми комп'ютерної телефонії історично були сконцентровані в центрах обробки викликів (Call-центрах), спочатку орієнтованих тільки на розподіл вхідні дзвінки, а потім обслуговуючих, як вхідну, так і вихідну навантаження.

Гарі Ньютоном, відомим фахівцем в області телекомунікацій, був введений термін комп'ютерна. В його словнику «Ньютонівські словник з телекомунікацій», дається таке визначення: Комп'ютерна телефонія (CT, Computer Telephony) – дисципліна використання розвинених логіко-

інформаційних можливостей комп'ютера для створення та прийому телефонних дзвінків, повідомлень факсимільного зв'язку та інших складних повідомлень і транзакцій за участю мереж загального користування, приватних мереж і мережі Інтернет. Цей термін охоплює безліч технологій, у тому числі, інтеграцію комп'ютер-телефон через локальну мережу, інтерактивну обробку мови, голосову пошту, операторські Call-центри, розпізнавання мови, перетворення текст мова, факсимільний зв'язок, одночасну передачу мови і даних, обробку мовних сигналів, відео конференції, автоматичний набір номера, аудіо текст, голосове відтворення даних, довідкові служби і багато інших технологій, що доповнюють і розширюють функціональні можливості традиційної телефонної комутації.

Проте найбільш розгорнуте визначення запропоновано провідною в цій області компанією Dialogic: Комп'ютерна телефонія – це технологія, яка дозволяє скоординувати дії телефонної та комп'ютерної системи для виконання наступних функцій:

– Прийом телефонного дзвінка, коли система виявляє вхідний виклик, відтворює (без участі оператора) голосову інформацію і меню опцій, а також дає можливість абоненту залишити своє повідомлення.

– Управління набором номера, коли абонент, набравши телефонний номер системи комп'ютерної телефонії, отримує пропозицію ввести з клавіатури телефону свій ідентифікаційний номер, а після верифікації цього номера отримує другий сигнал відповіді станції і вказівки про наступний крок, наприклад, міжміського або міжнародного номера.

– Автоматичне роз'єднання системами комп'ютерної телефонії, що відповідають на виклики шляхом відтворення записаної інформації (наприклад, прогнозу погоди), після закінчення її відтворення.

– Маршрутизація телефонного дзвінка (при цьому з апарата, що безпосередньо прийняв виклик, відповідь на виклик не відбувається). У варіанті програмованої переадресації вхідний телефонний виклик направляється до іншого телефонного номеру (наприклад, система мовних повідомлень дозволяє

користувачам заздалегідь вказати телефонний номер, до якого за їх відсутності на робочому місті повинні переадресовуватися вхідні дзвінки). Інший варіант автоматичної переадресації дозволяє відповісти на вхідний виклик і направити його до іншого розширення в разі, якщо від абонента не надходить жодних вказівок. Наприклад, прийнявши вхідний дзвінок, система комп'ютерної телефонії інструктує абонента: «набрати 1 у випадку, якщо виклик проводиться з кнопкового телефону, або почекати з'єднання ». Якщо абонент не набирає потрібний номер протягом 5 секунд, виклик автоматично переводиться до секретаря. Варіант переадресації в залежності від інформації, що надійшла від абонента: система відповідає на вхідний виклик і пропонує абонентові набрати, залежно від мети дзвінка, ту чи іншу комбінацію цифр. Наприклад, система комп'ютерної телефонії пропонує набрати 1 для з'єднання з відділом продажу, 2 - з відділом обслуговування і т.п., або зачекати відповіді секретаря. Ще один варіант - маршрутизація до служб телефонних аудіоконференцій, що дають абонентам можливість приєднуватися до бесіди двох або більше сторін, набираючи певну комбінацію цифр в режимі багаточастотного набору.

– Організація очікування: виклик перебуває у черзі до тих пір, поки особа яку викликають не зможе на нього відповісти, або поки не звільниться вихідна лінія, за якою може бути вироблена його подальша маршрутизація. Якщо кількість вхідних викликів перевищує кількість людей, що їх обслуговують, може бути організовано очікування відповіді. Абоненти що чекають зазвичай чують звуковий сигнал або голосове повідомлення, яке інформує їх про перспективи подальшого очікування, а наприклад, «телефон довіри», дозволяє абонентам одержувати в цей час безкоштовну інформацію, консультацію або допомогу.

– Надання інформації відповідно до меню опцій, що пропонується під час вступу до системи вхідного дзвінка. Абонент обирає потрібну опцію, натискаючи на певну кнопку телефонної клавіатури або просто називаючи обрану опцію (якщо система обладнана функцією розпізнавання голосу). Наприклад, служба «банківські операції з телефону »відповідає на дзвінок і

відтворює меню пропонованих послуг приблизно за такою моделлю: «Якщо вас цікавить стан рахунку, наберіть 1, якщо процентна ставка, наберіть 2 і т.п.» Інформація може відтворюватися автоматично або в залежності від обраної абонентом опції меню. Користувач може регулювати швидкість і гучність відтворення, набираючи відповідні комбінацію цифр.

– Отримання інформації, тобто запис і зберігання в комп'ютерному файлі для подальшої її обробки, що надходить від абонентів. Наприклад, система масового опитування респондентів, що працює за наступною схемою: люди телефонують по визначеному номеру, і їм пропонується записати свої міркування по обговорюваній темі. Інший варіант – визначення телефонного номера абонента за допомогою АВН. Наприклад, програмне забезпечення телемаркетингу може направити виклик до торгового агенту і в процесі його розмови з абонентом помістити в базу даних телефонний номер цього абонента та інформацію про запиті. Ще один варіант – фіксація набраної абонентом цифрової комбінації: реєструються і сортуються цифрові коди, набрані абонентами. Наприклад, автоматизована система проведення опитувань пропонує людям подзвонити за вказаним номером і проголосувати, вибравши ту чи іншу відповідь шляхом набору на телефонному апараті заданого цифрового коду. Система реєстрації визначає і записує інформацію про вхідні та вихідні телефоні виклики, включаючи дані про тривалість розмови, про дату і часу, набраний номер телефону або телефонний номер абонента і т.п. Це дозволяє, наприклад, оцінити продуктивність праці операторів телемаркетингової компанії, визначити середній час, що витрачається ними на роботу з одним телефонним викликом.

– Розпізнавання голосу дозволяє абонентам взаємодіяти з системами комп'ютерної телефонії, вимовляючи визначені слова або фрази. Ці технології особливо корисні в умовах, коли застосування багато частотного режиму набору номеру вельми обмежене. Система розпізнавання усних команд, що вимовляються певною людиною, передбачає індивідуальне налаштування системи комп'ютерної телефонії на конкретного користувача шляхом: (1)

формування списку слів, що вживаються (2) багаторазового аудіозапису цих слів, що дозволяє системі запам’ятати характеристики мови особи що відповідає(3) повторення запису в різних умовах (скажімо, при шумових перешкодах на телефонній лінії). Система розпізнавання усних команд незалежно від індивідуальних мовних особливостей мовця зазвичай передбачає вельми обмежений запас слів (цифри від 0 до 9), слова «так» і «ні» і т.д.

– Мережеві функції, до яких відносяться генерація і детектування зуммерних сигналів ТМЗК, що дозволяє програмі зробити виклик і вести потім моніторинг процесу його обслуговування. Поряд з генерацією стандартних зуммерних сигналів ТМЗК при наборі телефонного номера абонентами, можлива генерація й детектування нестандартних акустичних одночастотних і двочастотних сигналів з амплітудою і тривалістю,що не використовуються у звичайній практиці ТМЗК.

Отже можна сказати що комп’ютерна телефонія – це технологія надання послуг на базі об’єднання комунікаційних можливостей телефонних систем і обчислювальних можливостей та ресурсів баз даних комп’ютерних систем. Яскравим прикладом комп’ютерної телефонії, що часто зустрічається в житті людини є Call-центр, особливо його головній модуль - система IVR.

1.2 Call центр

Саме поняття Call-центр з’явилося досить давно. Ще в 60-і роки минулого століття. І тоді це були великі операторські служби, які відповідали на велику кількість дзвінків. В даний час на ринку існують рішення, які орієнтовані на компанії будь-якого розміру, різні за можливостями і в різному ціновому діапазоні. Call-центр компанії - це, в першу чергу, група підготованих і постійно контрольованих людей, які обслуговують дзвінки клієнтів. В правильно організованому Call-центрі, дзвінок, що надходить, спочатку направляється в IVR меню, а вже далі, якщо необхідна інформація не була надана клієнту в процесі його взаємодії з системою, виклик, безпосередньо, надходить до оператора, або вибраного відділу компанії (рисунок 1.1).

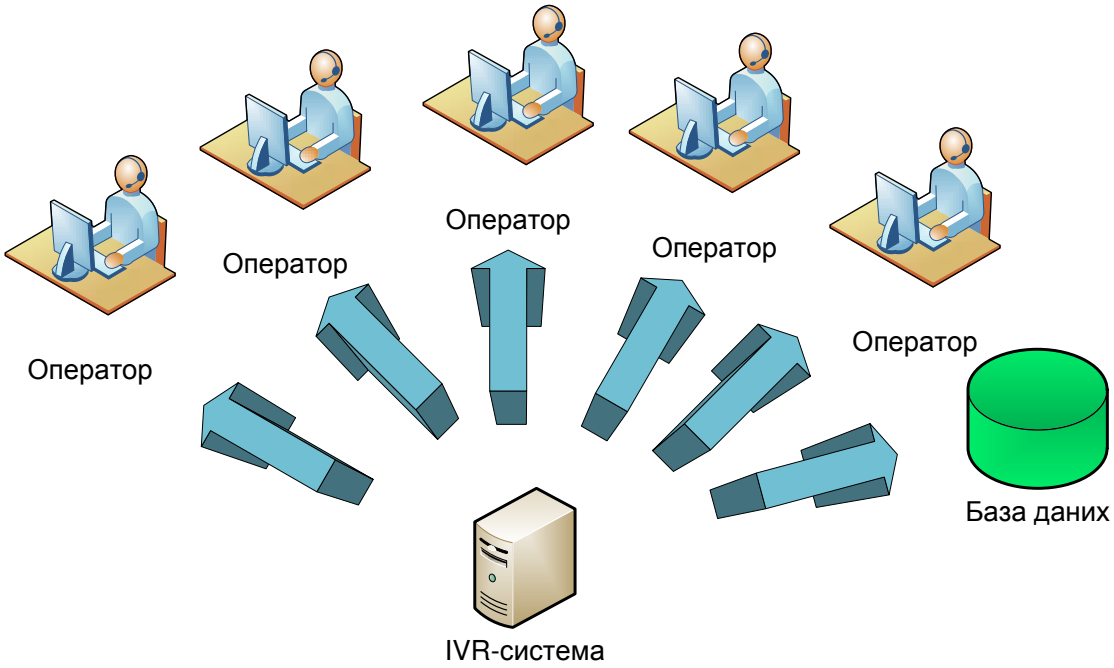

Рисунок 1.1 – Структурна схема Call-центру

Існує кілька способів, що дозволяють компанії організувати роботу зі своїми клієнтами у форматі Call-центру. Який спосіб вибрати - компанія визначає відповідно до своїх поточних потреб і планів на майбутнє. Необхідність у створенні Call-центру, як для компаній великого бізнесу, так і для компаній малого і середнього бізнесу, обґрунтована хоча б тим, що клієнти потрібні всім компаніям, незалежно від їх розміру. А Call-центр є надійним і гарантованим засобом збереження й збільшення бази клієнтів компанії при адекватних витратах на цей процес.

До найбільш типових для Call-центру бізнес-процесів належать такі, як обробка контактів сервісної служби, прийом претензій від споживачів або замовлень по телефону, пошук нових клієнтів шляхом вихідних дзвінків та розсилання комерційних пропозицій, опитування клієнтів компанії, відповіді на питання по рекламним акціям, що проводяться і т.д.

Технічно Call-центр являє собою комплекс, що включає наступні компоненти:

– Телефонні канали;

– Телефонну станцію з можливістю ведення реєстрів операторів (або агентів), розподілу дзвінків (ACD – Automatic Call Distribution) на основі їх параметрів і навичок операторів (skillsets) і т. п.;

– Внутрішню телекомунікаційну мережу;

– Робочі місця операторів, обладнані телефонними апаратами і ПК для роботи з інформаційною системою;

– Робочі місця супервізорів (для контролю операторів і моніторингу статистики в режимі реального часу);

– Інформаційну систему. Як правило, вона включає базу необхідних операторам знань, а також CRM для ведення історії контактів і збору даних про клієнтів і є інтегрована з телефонною системою.

Але в силу розвитку технологій, звичайного обслуговування телефонних дзвінків вже недостатньо, з'явилось багато інших видів зв'язку, наприклад електронна пошта, IP телефонія, відео конференції та інше. Тому все частіше Call-центр є лише частиною, нової, більш функціональної системи під назвою контакт-центр.

1.3 Контакт-центр

Контакт-центр – це структура, що складається з програмно-апаратного комплексу та операторського центру (Call-центр) обробки звернень по всіх відомих каналах зв'язку (рисунок 1.2).

Застосовуються два основних види центрів обробки викликів: власні і аутсорсингові.

Для того щоб створити власний контакт-центр компанії необхідно придбати досить дороге обладнання, спеціалізовані меблі, провести телефонні канали, навчити операторів.

При цьому компанія отримує можливість повністю контролювати роботу центру обробки викликів. Це важливо в тих випадку, коли інформація, до якої мають доступ оператори, конфіденційна, і її не можна довірити сторонньому центру обробки викликів (банки, деякі фінансові організації). Або ж оператори

вимагають надто складної підготовки. Наприклад, для медичних організацій простіше навчити людину з медичною освітою навичкам спілкування по телефону, ніж оператора медичним знанням.

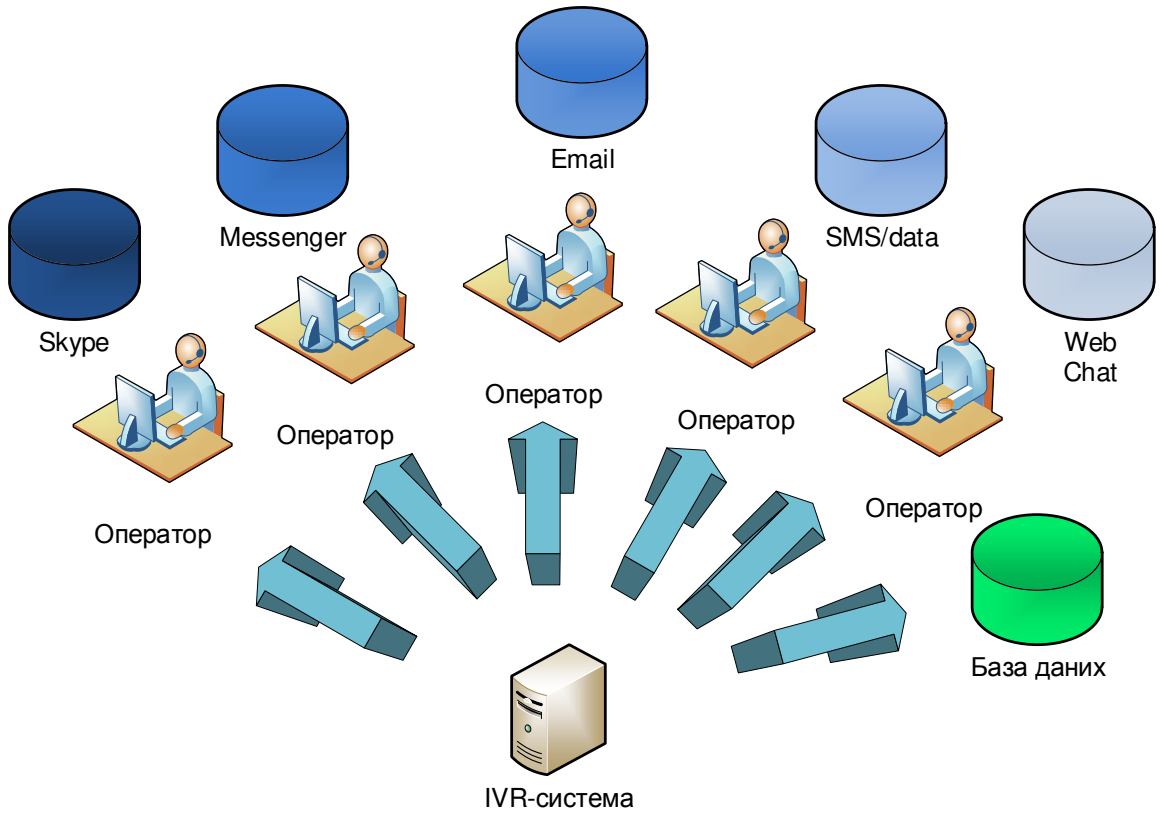

Рисунок 1.2 – Структурна схема контакт центру

Через високі стартові витрат, звичайно, не має сенсу організовувати контакт-центр для обробки невеликої кількості дзвінків і для разових рекламних акцій. Таким чином, якщо компанія, з якихось причин не бажає звертатися до аутсорсинговий контакт-центр, як правило, вона зовсім відмовляється від використання контакт-центру, що зменшує успіх акцій і змушує зовсім відмовитися від деяких з них.

Для разових рекламних акцій або для типових завдань часто користуються послугами аутсорсингового контакт-центру. Звернення в такий контакт-центр обійдеться в межах 25000 грн. в місяць, при цьому компанія-замовник звільнена від необхідності утримувати штат операторів та організовувати їх роботу. Однак, переваги цього способу для одних випадків

обертаються недоліками в інших випадку. Це недостатня конфіденційність, недостатні знання операторів, відсутність зворотного зв’язку від клієнтів.

Перевагами зовнішнього (аутсорсингового) контакт-центру є:

– низькі стартові витрати;

– швидкий старт;

– низька вартість контакт-центру з невеликою кількістю операторів;

– низькі витрати при низькому навантаженні;

– більше видів сервісу.

Недоліками зовнішнього (аутсорсингового) контакт-центру є:

– можливі витоку інформації, бази клієнтів, можуть стати надбанням громадськості якісь факти, які компанія не хотіла б розголошувати;

– ризик фіктивних рахунків;

– погіршується зворотній зв’язок, менше інформації про те, з якими питаннями звертаються клієнти;

– нижча якість обслуговування за рахунок менших знань оператора про певну предметну область.

Види діяльності, яким у силу їх специфіки більше підходить звернення до зовнішніх контакт-центрів: разові рекламні акції; пробні контакт-центри; компанії, які не можуть заздалегідь оцінити навантаження; телемаркетинг.

Звернутися в зовнішній контакт-центр дешевше, ніж створювати свій власний, але він обходиться дорожче під час роботи. Тому, звичайно компанії звертаються до зовнішніх контакт-центрам для коротких рекламних акцій або при обмеженому бюджеті. Також популярні звернення "щоб спробувати", оцінити ефект, навчитися.

Надалі, при бажанні компанії працювати з клієнтами через Call-центр на постійній основі, стає вигідною організація власного контакт-центру.

Переваги свого контакт-центру:

– безпека корпоративної інформації;

– можливість обробки дзвінка висококваліфікованими операторами, що володіють специфічними знаннями;

– контроль, впевненість у надійності;

– тісний зв’язок з клієнтом;

– більш грамотне обслуговування, спеціалізовані оператори.

Недоліки свого контакт-центру:

– високі витрати на старт;

– високі витрати на утримання;

– витрати на підготовку операторів, пошук кадрів;

– складності з розширенням, особливо при необхідності придбання додаткових каналів зв’язку;

– потрібен персонал для організації чергування, адміністрування;

– необхідність придбання своїх каналів зв’язку.

Види діяльності, яким у силу їх специфіки більше підходять власні контакт-центри: банки, аптеки, дуже великі компанії, компанії, що вимагають специфічних знань від операторів, що мають дуже багато дзвінків.

Головним недоліком власного Call-центру можна вважати вартість його створення, значну частину якої становлять витрати на обладнання та канали зв’язку.

Лінії зв’язку в контакт-центрах завжди багатоканальні, для того, щоб обслужити достатньо велику кількість дзвінків та інших запитів. Найчастіше для цього застосовуються серійні лінії, PRI-канали або Інтернет.

Серійна лінія представляє собою звичайні 4-5 телефонних ліній з одним загальним номером. При цьому міська АТС настроюється таким чином, що при зайнятій першій лінії дзвінок надходить на другу, при зайнятій другий – на третю і так далі. Недоліки: слабка розширюваність (4-5 ліній часто є межею); простий перебір не дозволяє регулювати навантаження на оператора.

PRI-канали

PRI – це стандарт, який використовується для підключення офісів. Він використовує для передачі інформації канал T1 в США, і канал E1 для Європи. Канал T1 PRI містить у собі 24 каналу, E1 PRI - 32 каналу. У Європі PRI-канал іноді називають просто лінією E1. PRI-канал являє собою кабель, по якому

телефонна станція може подати до 30 телефонних розмов одночасно. Недоліки – необхідне спеціальне обладнання щоб прийняти такі дзвінки; такого кабелю часто не виявляється в офісній будівлі. У цьому випадку його прокладання може зайняти значного часу і грошових витрат, а при переїзді цей процес доведеться повторити і оплатити знову.

IP-телефонія

Сучасні технології дозволяють організувати зв'язку по мережі Інтернет. Цей зв'язок відноситься до IP-телефонії. IP-телефонія – це технологія, яка пов'язує воєдино переваги телефонії та Інтернету. До недавнього часу мережі з комутацією каналів (телефонні мережі) і мережі з комутацією пакетів (IP-мережі) існували практично незалежно одна від одної і використовувалися для різних цілей. Телефонні мережі використовувалися тільки для передачі голосової інформації, а IP-мережі – для передачі даних. Технологія IP-телефонії об'єднує ці мережі за допомогою пристрою, що називається шлюзом або gateway. Шлюз являє собою пристрій, в який з одного боку включаються телефонні лінії, а з іншого боку – IP-мережа (наприклад, Інтернет).

У загальних рисах передача голосу в IP-мережі відбувається таким чином. Вхідний дзвінок і сигнальна інформація з телефонної мережі передаються на прикордонний мережевий пристрій, який називається телефонним шлюзом, і обробляються спеціальною картою пристрою голосового обслуговування. Шлюз, використовуючи керуючі протоколи сімейства SIP (SIP (англ. Session Initiation Protocol – протокол встановлення сесії) – стандарт на спосіб встановлення і завершення користувацького Інтернет-сеансу, що включає обмін мультимедійним вмістом (відео- і аудіоконференція, миттєві повідомлення, онлайн ігри). У моделі взаємодії відкритих систем SIP є мережним протоколом прикладного рівня.), перенаправляє сигнальну інформацію іншому шлюзу, що знаходиться на приймальній стороні IP-мережі. Приймальний шлюз забезпечує передачу сигнальної інформації на приймальне телефонне обладнання згідно з планом номерів, гарантуючи скрізне з'єднання. Після встановлення з'єднання голос на вхідному мережевому пристрої оцифровується (якщо він не був

цифровим), кодується відповідно до стандартних алгоритмами ITU, такими як G.711 або G.729, стискається, інкапсулюється у пакети і відправляється за призначенням на віддалений пристрій з використанням стека протоколів TCP/IP. Прихожі на приймальний шлюз IP-пакети перетворюються назад в телефонний сигнал і приймаючий абонент отримує виклик.

Оскільки при IP-телефонному дзвінку ніяк не задіяний міжнародний (міжміський) телефонний оператор, вартість цього дзвінка на порядок менше вартості традиційного телефонного з'єднання.

Проте дзвінок Телефон-Телефон є найочевиднішим, але далеко не єдиним сервісом, який може надавати оператора IP-телефонії. Використовуючи IP-мережу, можна обмінюватися цифровою інформацією для пересилання голосових або факсимільних повідомлень між двома комп'ютерами в режимі реального часу. Застосування Internet дозволить реалізувати дану службу в глобальному масштабі. Для IP-телефонії найчастіше використовується стандарт SIP, що визначає передачу відео та аудіо по мережах з негарантованою якістю послуг, таких як Ethernet і IP. SIP описує кілька елементів, у тому числі аудіо та відео кодеки (кодери / декодери), комунікаційні протоколи і синхронізацію пакетів[6].

Переваги IP-телефонії

Здешевлення телефонних переговорів. Впровадження технології VoIP в рамках обчислювальної мережі дозволяє зменшити сумарні витрати, пов'язані з веденням міжнародних і міжміських телефонних переговорів, а також розпочати процес міграції до технологій пакетної передачі мультимедійних даних. Крім того, з огляду на можливість виходу на міську телефонну мережу, використання цієї технології може звести до мінімуму оренду звичайних телефонних ліній.

VoIP (англ. Voice over IP; IP-телефонія) – система зв'язку, що забезпечує передачу мовного сигналу мережею Інтернет або будь-якими іншими IP-мережами. Сигнал по каналу зв'язку передається в цифровому вигляді та, як

правило, перед передачею перетворюється (стискується) для того, щоб видалити надмірність.

Покращена якість зв’язку

Якість зв’язку можна оцінити, використовуючи наступні основні характеристики: рівень спотворення голосу; частота «зникнення» голосових пакетів; час затримки (між виголошенням фрази першого абонента і моментом, коли вона буде почута другим абонентом). По всім перерахованим характеристикам якість зв’язку значно збільшилась в порівнянні з першими версіями рішень IP-телефонії, які допускали спотворення і переривання мови. Поліпшення кодування голосу і відновлення втрачених пакетів дозволило досягти рівня, коли мова розуміється абонентами настільки добре, що співрозмовники не здогадуються, що з’єднання відбувається за технологією IP-телефонії. Зрозуміло, що затримки впливають на темп бесіди. Відомо, що для людини затримка до 250 мілісекунд практично непомітна. Існуючі на сьогоднішній день рішення IP-телефонії не перевищують цю межу, так що розмова фактично не відрізняється від зв’язку по звичайній телефонній мережі. Крім цього, затримки зменшуються завдяки наступним трьом факторам:

– По-перше, удосконалюються телефонні сервери (їх розробники борються із затримками, покращуючи алгоритми роботи);

– По-друге, розвиваються приватні (корпоративні) мережі (їх власники можуть контролювати ширину смуги пропускання і, отже, величини затримки);

– По-третє, розвивається сама мережа Інтернет - сучасний Інтернет не був розрахований на комунікації в режимі реального часу. The Internet Engineering Task Force (IETF) разом з операторами мереж Інтернет пропонують нові технології, такі, як Reservation Protocol (RSVP), які дозволяють резервувати смугу пропускання.

Підвищення якості факсимільного зв’язку.

Так як, по суті факсимільне повідомлення – потік цифрових даних, а в технології VoIP дані передаються в цифровому вигляді, тому передача факсимільних повідомлень по аналогових ліній скорочується до мінімуму. А за

рахунок того, що обладнання має можливість демодульованого сигнал перед передачею по IP-мережі і передавати закодоване в 64Кбітном форматі факс-повідомлення в смузі 9,6 Кбіт, знижується навантаження на канали.

Інтеграція філій в єдину інформаційну структуру. Останнім часом з розвитком інформаційних технологій та збільшенням пропускної здатності каналів все для найбільш оперативного вирішення ділових завдань філії компанії об'єднують в одне ціле, утворюючи інтрамережі. Так як пропонована технологія використовує для передачі голосу мережі передачі даних, то з'являється можливість об'єднувати не тільки комп'ютерні мережі, але й телефонні.

Віртуальні приватні мережі (VPN). IP-телефонія є ідеальною технологією для побудови віртуальних приватних мереж підприємства. Головна риса технології VPN - використання IP-мережі як магістралі для передачі корпоративного IP-трафіка. Мережі VPN вирішують завдання підключення корпоративного користувача до віддаленої мережі та з'єднання декількох віддалених ЛОМ та АТС в єдину корпоративну мережу передачі голосу і даних.

Глобальний роумінг. IP-телефонія дозволяє операторам зв'язку дуже просто і з мінімальними витратами організувати роумінг послуг зв'язку. Це особливо актуально для операторів мобільного зв'язку - рішення, побудоване на технологіях IP-телефонії, на порядок дешевше традиційного, і володіє набагато більшою гнучкістю.

Суміщений доступ в Інтернет. Голосові дані, факсимільні повідомлення передаються з використанням IP - основного набору протоколів Інтернет, дане рішення само собою має на увазі доступ до ресурсів Мережі і очевидна економія на оренду ліній зв'язку та оплату послуг[6].

GSM-шлюзи і CDMA-шлюзи

Для підключення мобільних номерів GSM-і CDMA-зв'язку застосовуються відповідно GSM-шлюзи і CDMA-шлюзи. GSM-шлюз – це невеликий пристрій, що забезпечує пряме з'єднання корпоративної телефонної системи з мережею GSM. Оскільки оператори мобільного зв'язку пропонують

спеціальні тарифи для дзвінків всередині мережі, GSM шлюз здатний у багато разів скоротити витрати на з'єднання за рахунок внутрішньомережевої тарифікації.

Таким чином, GSM-шлюз можна вважати мобільним телефоном, підключеним до стаціонарної мережі загального користування. Тільки доступ до нього відбувається через офісну мережу.

Керівництво компаній, які встановили у себе GSM-шлюзи приємно дивує їхня швидка окупність. Навіть при порівняно невеликій кількості вихідних дзвінків (близько 5 годин на місяць на одну особу), GSM-шлюз окупається максимум за два місяці. Хоча практика показує, що цей термін може бути набагато менше.

У різних режимах роботи обслуговуваних шлюзом клієнтів економія на дзвінках може досягати 70-80%!

Також, використовуючи шлюзи, можна вільно проектувати телефонні лінії у віддалених районах, куди немає можливості протягнути звичайну дротову телефонію, але є стійкий сигнал GSM. Достатньо підключити до шлюзу один або кілька стаціонарних телефонних апаратів або міні-АТС і офіс, квартира або заміський будинок телефонізовані.

Принцип роботи CDMA-шлюзу аналогічний принципу роботи GSM-шлюзи.

Офісна АТС-телефонна станція, що обслуговує дзвінки одного або декількох установ або організації. Бувають аналоговими, цифровими та IP-телефонії. Аналогові вже практично не застосовуються через їх обмеженої функціональності, часто вже не задовольняє потреби сучасних офісів. Цифрові - більш сучасні, але й вони витісняються найбільш сучасними IP-телефонними станціями. IP-телефонні станції мають на сьогодні найменшу ціну каналу при найбільших функціональних можливостях та можливості розширення.

Варто відмітити, що жоден контакт-центр не обходиться без CRM-системи, яка забезпечую біль повну взаємодію з клієнтами, завдяки її спеціальним модулям і тісним зв'язком з інформаційним середовищем

організації і партнерських підприємств. Але й в CRM-системах, які використовуються в контакт-центрах, IVR система залишається головним модулем, завдяки якому здійснюється збір необхідної інформацій про клієнта, шляхом аналізу даних про звернення[7].

1.3 CRM-системи

Кожна компанія, вибудовуючи свій бізнес, на певному етапі розвитку реалізує стратегію поведінки стосовно своїх клієнтів.

Ця стратегія повинна бути заснована на використанні передових управлінських і інформаційних технологій, за допомогою яких компанія збирає інформацію про своїх клієнтів на всіх стадіях його життєвого циклу (залучення, утримання, лояльність), отримує з неї знання і використовує ці знання на користь свого бізнесу шляхом вибудовування взаємовигідних відносин з ними.

Результатом застосування стратегії є підвищення конкурентоспроможності компанії і збільшення прибутку, тому що правильно побудовані відносини, засновані на персональному підході до кожного Клієнта, дозволяють залучати нових клієнтів та допомагають утримати старих.

Система управління взаємодією з клієнтами (скор. від англ. Customer Relationship Management System, CRM-система) – корпоративна інформаційна система, призначена для автоматизації CRM-стратегії компанії, зокрема, для підвищення рівня продажів, оптимізації маркетингу та поліпшення обслуговування клієнтів шляхом збереження інформації про клієнтів (контрагентів) та історії взаємин з ними, встановлення і поліпшення бізнес-процедур і подальшого аналізу результатів.

Системи стандарту CRM призначені для підтримки та забезпечення наступних функцій:

- Збір інформації про Клієнта;
- Аналіз і висновки на базі цієї інформації;
- Експорт інформації в інші системи;
- Підтримка відносин з Клієнтом.

Програмні рішення CRM дозволяють відслідковувати розвиток взаємин із замовниками, координувати відносини з постійними Клієнтами та здійснювати централізоване управління продажами, в тому числі і через Інтернет.

– Таким чином, CRM-системи забезпечують оперативний доступ до інформації і використовуються для аналізу таких завдань, як:

– Оперативні (забезпечують оперативний доступ до інформації);

– Аналітичні (використовуються для аналізу різних даних, які відносяться як до Клієнта, так і до діяльності фірми);

– Завдань по співпраці (надають клієнтам можливість більшого впливу на діяльність компанії, в тому числі й на процеси розробки дизайну, поряд з процесами виробництва, доставки та обслуговування продукту).

Впровадження CRM-системи позначається на роботі майже всіх підрозділів фірми, а не тільки відділу продажів, і вимагає тісної інтеграції з іншими інформаційними системами.

Сучасні CRM-системи які використовуються в контакт-центрах забезпечують комплексний підхід до автоматизації роботи з клієнтами та спрямовані на надання максимально зручного для споживача сервісу. Одним з найважливіших завдань систем цього рівня є організація взаємодії між підрозділами маркетингу, продажів і сервісного обслуговування. За статистикою, ці теми найчастіше цікавлять клієнтів при зверненні в контакт-центри.

До засобів автоматизації (програмного забезпечення) CRM відносяться:

– Програмно-апаратні рішення для Call-центрів;

– Системи управління взаємодією з клієнтами (CRM-системи);

– Системи технічної підтримки зовнішніх і внутрішніх замовників (системи класу Service Desk)[8].

1.4 Програмно-апаратний комплекс IVR

Безумовно, сьогодні як ніколи компанії прагнуть до підвищення якості обслуговування клієнтів і вдосконалення своєї телефонної інфраструктури.

IVR (Interactive Voice Response – інтерактивний голосова відповідь) – система інтерактивної голосової взаємодії, в якій користувач може отримати доступ до інформації, яка його цікавить, використовуючи спеціальне голосове меню, керуючи ним за допомогою натиснення клавіш в тоновому режимі або за допомогою голосу (при використанні технологій розпізнавання голоси).

Крім того, IVR-система, є стартовою точкою для клієнта при зверненні до контакт-центру (риснок 1.3).

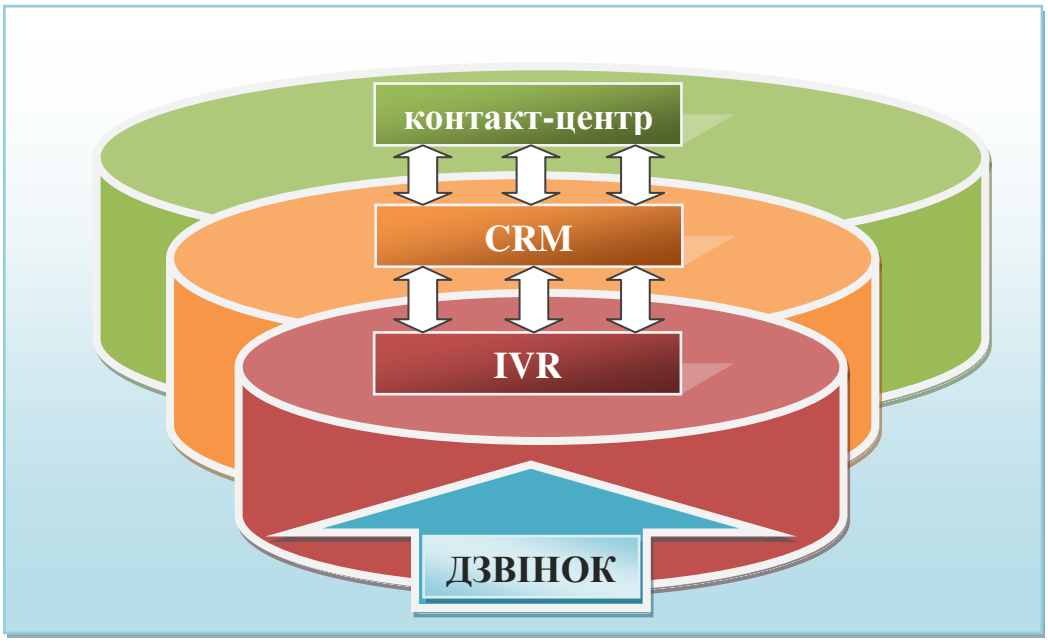

Рисунок 1.3 – Звернення клієнту до контакт –центру

Залежно від моделі представлення інформації розрізняють системи статичного і динамічного IVR.

Статичний IVR заснований на голосовому меню, в якому користувачеві надається строго певна кількість даних у вигляді попередньо записаних голосових повідомлень. Статичний IVR досить простий в реалізації. Найбільш часто використовується для привітання при дозвоні в компанію, а також програвання рекламних та інформаційних повідомлень під час очікування в черзі.

Динамічний IVR дозволяє використовувати данні, що постійно змінюються, поряд з попередньо записаними голосовими повідомленнями.

Наприклад, абонент може отримувати довідку про поточний стан свого рахунку або про актуальний курс валют. Отримання інформації в даному випадку здійснюється за рахунок інтеграції системи IVR з базами даних компанії, а подання проводиться відповідно до розроблених правил маршрутизації.

Вартість реалізації IVR-системи на базі цих методів може відрізнятися на декілька порядків. Як показує практика, при виборі IVR на підставі цінових характеристик, як правило, віддається перевага саме статичному IVR, але в процесі своєї діяльності компанія досить швидко доходить до потреби підвищення функціональності.

Системи IVR можуть використовуватися як з незалежною АТС, так і з call-центром компанії. В обох випадках IVR може виконувати функції маршрутизації, але, як правило, економічно виправданим використання IVR-систем є саме у другому випадку. При великій кількості звернень до call-центру компанії IVR може забезпечити раціональне завантаження операторів в залежності від їх спеціалізації, що дозволить зменшити кількість перенаправлень і час обробки дзвінка.

Крім маршрутизації на IVR можуть покладатися функції інформаційної служби, прийому заявок, телеголосування, автоматичного обдзвону і т.д.

Використання IVR найбільш доцільно в тих галузях, де здійснюється масове обслуговування клієнтів. Як правило, в такому випадку більшість звернень є стандартизованими, що спрощує використання IVR-систем. На базі IVR може бути побудована цілодобова інформаційна підтримка клієнтів та уточнення певної конфіденційної інформації.

У той же час, використання IVR повинно виправданим з позиції клієнта і компанії. Для того, що б побудувати раціональну систему обслуговування на базі IVR необхідно, як мінімум, чітко представляти потреби клієнта, специфіку інформації та "цінність" клієнта для компанії. Так, наприклад, мобільні оператори більшість запитів абонентів передплаченого зв’язку переадресовують на IVR. При зверненні представника великого корпоративного клієнта йому, з високою часткою ймовірності, відразу

відповість оператор call-центру, а vip-клієнта при цьому привітають на ім’я й по батькові. Крім того, вже зустрічаються приклади, коли при формуванні IVR-меню може враховуватися рівень професійної компетенції клієнта і т.п.

У банківському секторі, як правило, за допомогою IVR обслуговуються близько 30% усіх звернень, а у сфері телекомунікацій цей показник може досягати і 60%.

На жаль, навіть у разі побудови оптимальної IVR-системи на початковому етапі, практично не можна гарантувати її ефективність у подальшому. Поява нових масивів інформації вимагає зручного інструментарію та якісного адміністрування. Структура меню та форма подачі інформації повинна постійно аналізуватися і, в разі необхідності, доопрацьовуватися. У такій ситуації збір даних про переваги чи недоліки IVR-системи (з точки зору конкретного користувача) і зміни в перевагах клієнта доцільно здійснювати в CRM-системі, а оперативний аналіз проводити за допомогою операційного BI.

1.5 Призначення IVR

Підвищення якості обслуговування клієнта

Бажання кожного абонента клієнта – швидко отримати ясну відповідь на своє запитання. Застосування системи IVR дозволяє зменшити час очікування в черзі на обслуговування. Дослідження показують, що близько 40% питань клієнтів досить прості і можуть бути легко автоматизовані, при цьому оператори зможуть зосередитися на обслуговуванні більш складних

клієнтських запитів. В результаті автоматизації відповідей на прості запитання скоротиться час очікування з’єднання з оператором і зменшиться число абонентів, що не дочекалася відповіді.

Використання системи IVR дозволяє цілодобово обслуговувати клієнтів без залучення для цієї мети додаткового персоналу.

Збільшення доходу компанії

Перехід на цілодобовий режим обслуговування дзвінків сприяє зростанню клієнтської бази, що, відповідно, збільшує доходи компанії. Також є можливість розширення ринку продажів за рахунок залучення абонентів з

інших часових поясів. Співробітники, які обслуговують клієнтів, звільняються від рутинної роботи і зосереджуються на більш важливих питаннях. Підвищується ефективність роботи персоналу.

Зниження накладних витрат

Тут простежується проста залежність: використання системи IVR дозволяє скоротити штат і таким чином зменшити витрати на зарплату, оренду приміщення, оплату телефонних переговорів, закупівлю та обслуговування додаткового обладнання

1.6 Архітектура IVR системи

1) Архітектура та вимоги до IVR-платформ

Сьогодні в IVR-платформах потребують великі корпорації, наприклад, мобільні оператори і сервіс-провайдери з абонентською базою в сотні тисяч і мільйони абонентів. У таких системах кількість каналів зв'язку складає десятки і сотні, а інтенсивність дзвінків досягає сотень і тисяч в хвилину.

Перспективи використання стандартної IVR-платформи визначаються її функціональністю, зокрема:

- можливістю створення голосових меню;
- доступом до протоколів для взаємодії із зовнішніми системами: корпоративними базами даних, SMS/USSD-центрами, системами адміністрування та відстеження працездатності системи;
- нарощуванням продуктивності за рахунок горизонтального масштабування системи, тобто збільшення кількості телефонних плат і / або транків (trunks) на них.

Сучасна IVR-платформа, крім перерахованих, повинна володіти наступними перевагами:

- відкрита структура меню і бізнес-логіка;
- надійність і безперервне обслуговування абонентів;
- коректне функціонування при відмові окремогокомпоненту і відновлення після збоїв;

– мінімальні зусилля з інтеграції існуючої телефонної інфраструктури та корпоративної бази даних.

Грамотно спроектована IVR-платформа надалі буде вимагати від розробника мінімальних зусиль з:

– розробки нових голосових додатків;

– підтримці нових джерел даних і протоколів;

– переходу на нове телефонне обладнання.

2) Архітектура IVR-платформи

Архітектура IVR-платформи повинна задовольняти наступним вимогам:

– бути багаторівневою (рисунок 1.4), щоб кожний рівень міг взаємодіяти з іншими за допомогою абстрактних, чітко визначених і мінімізованих інтерфейсів. Це забезпечить можливість швидко змінити рівень, не зачіпаючи інших (наприклад, для підтримки телефонного обладнання нового виробника);

– кожен рівень повинен складатися з замінних функціональних підсистем. На рисунку 1.5 представлені підсистеми та їх взаємодія на рівні бізнес-логіки. При виході з ладу однієї з підсистем така архітектура забезпечить захист IVR від зупинки – втративши частину функціональності, вона залишиться працездатною. При збої в будь-якій підсистемі IVR доступними засобами що залишились повинен інформувати адміністратора про проблему. Крім того, така організація дозволяє нарощувати функціональність IVR-платформи шляхом додавання нових підсистем на відповідному рівні, не зачіпаючи інших;

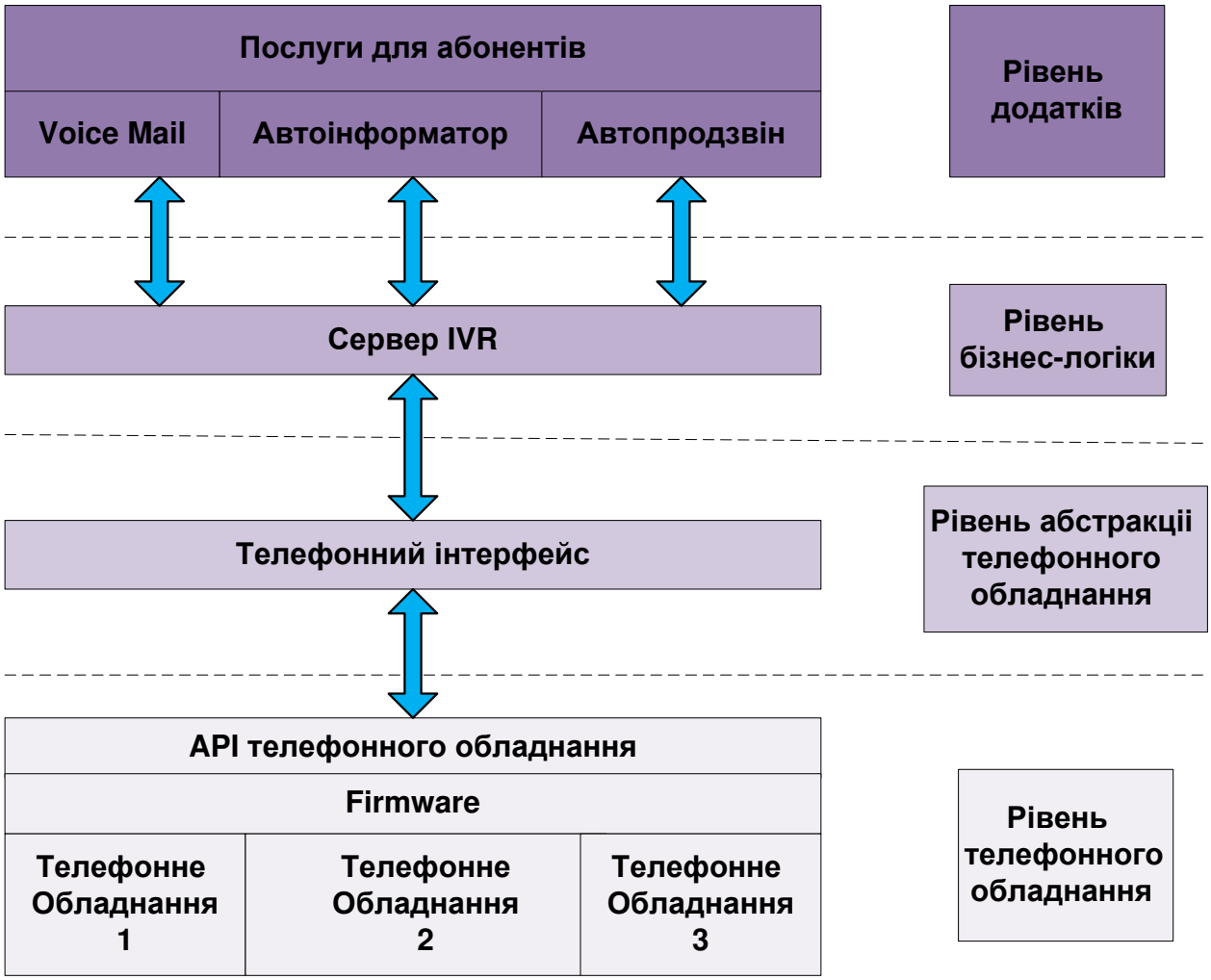

Рисунок 1.4 – багаторівнева архітектура IVR

– забезпечувати достатній рівень дублювання серверів або навіть мати можливість "гарячого" дублювання (при виході з ладу одного сервера резервний автоматично обробить всі активні дзвінки без розриву з’єднання і втрати інформації).

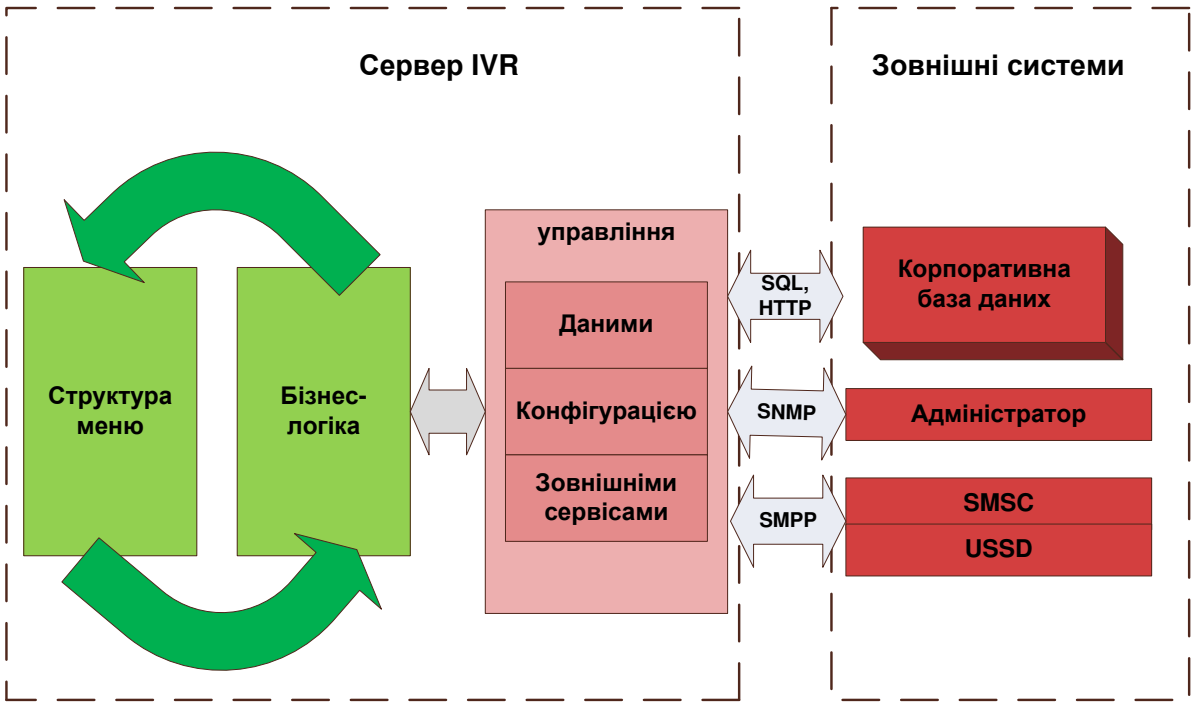

Рисунок 1.5 – рівень бізнес-логіки IVR

Вимоги до функціональності за рівнями

1.6.1 Рівень додатків

– Можливість для замовника самостійно змінювати структуру меню і бізнес логіку, що дозволить підрозділу, який відповідає за впровадження і супровід, самостійно виробляти необхідні доопрацювання.

– Динамічний розподіл фізичних телефонних ресурсів для голосових додатків. Наприклад, коли потрібно обдзвонити абонентів, IVR повинен надати автопрозвонщіку необхідні ресурси за рахунок скорочення ресурсів у інших програм, але таким чином, щоб не блокувати їх роботу.

– Складання фраз із голосових фрагментів на правильній мові, особливо якщо IVR підтримує декілька мов. Для узгодження текстів доцільно запросити носія мови, оскільки помилки у вимові викликають недовіру абонентів до всієї системи.

1.6.2 Рівень бізнес-логіки

– Отримання інформації про стан телефонних каналів, транків та бази даних в реальному часі для оперативного реагування на виникаючі проблеми.

– Статистика по дзвінках для формування звітів та локалізування проблем. Проблеми в телефонній або локальної мережі можуть носити короткостроковий характер, тому статистика повинна бути як мінімум похвилина. Якщо будувати менш точні графіки, наприклад, з десятихвилинною статистикою, то на них будуть згладжені спади і викиди, що сигналізують про можливу наявність проблем з обладнанням. Звіти зі статистикою можуть використовуватися і як аргумент на користь рішення про розширення системи.

– Можливість без переривання обслуговування абонентів зміни структури меню, бізнес-логіки і настройки параметрів системи.

1.6.3 Рівень абстракції телефонного обладнання

– Наявність інтерфейсу "рівня абстракції обладнання", що забезпечує використання будь-якої телефонної технології, так як телефонні протоколи можуть істотно відрізнятися по функціональності і способам встановлення з’єднання (наприклад, цифрові протоколи ISDN і протоколи 1P-телефонії).

– Підвищення продуктивності IVR за рахунок модернізації апаратної частини системи. При збільшенні кількості абонентів або появи нових голосових додатків навантаження на IVR систему зростає, яка при цьому не повинна вимагати доопрацювання програмної частини для підтримки горизонтального масштабування за рахунок збільшення числа телефонних плат і / або транків на них. Необхідність у нарощуванні продуктивності визначається емпіричним шляхом – досліджується структура дзвінків у конкретного оператора зв’язку на конкретну послугу. На рисунку 1.6 представлено добовий розподіл дзвінків до оператора мобільного зв’язку на автоінформатор на один ISDN PRI транк (30 каналів) у хвилину. У години найбільшого навантаження (ГНН) необхідно зробити статистично значуще кількість спроб додзвонитися на IVR, і якщо хоча б одна з них буде невдалою через зайнятість лінії, то

необхідно розширення обладнання, так як ненадання послуги викликає нарікання абонентів до оператора зв’язку.

– Обмеження тривалості дзвінка, щоб уникнути ситуацій, коли PBX не визначає розрив з’єднання і дзвінок залишається активним, незважаючи на те що абонент поклав трубку. Зазвичай це відбувається, коли виклик здійснюється з аналогових міських ліній.

– Зв’язок з оператором для вирішення питань, які абонент не хоче або не може вирішити за допомогою IVR. Це вимагає наявності в IVR перенаправлення (трансферу) дзвінка. Дана функціональність може бути реалізована використанням: трансферу, специфічного для конкретної телефонної станції (PBX Private Branch eXchange); стандартних типів трансферу; ресурсів самої телефонної плати. Ці рішення обумовлюють різні ступені інтеграції з конкретною PBX і перераховані згідно спаданню даної залежності. При використанні специфічної функціональності PBX або телефонної плати виникає залежність реалізації від технічної складової, що ускладнює можливість переносити системи. У IVR-платформі необхідно мінімізувати інтерфейс "рівня абстракції устаткування" і, як наслідок, використовувати в ній тільки стандартні функції телефонних протоколів та обробки голосу.

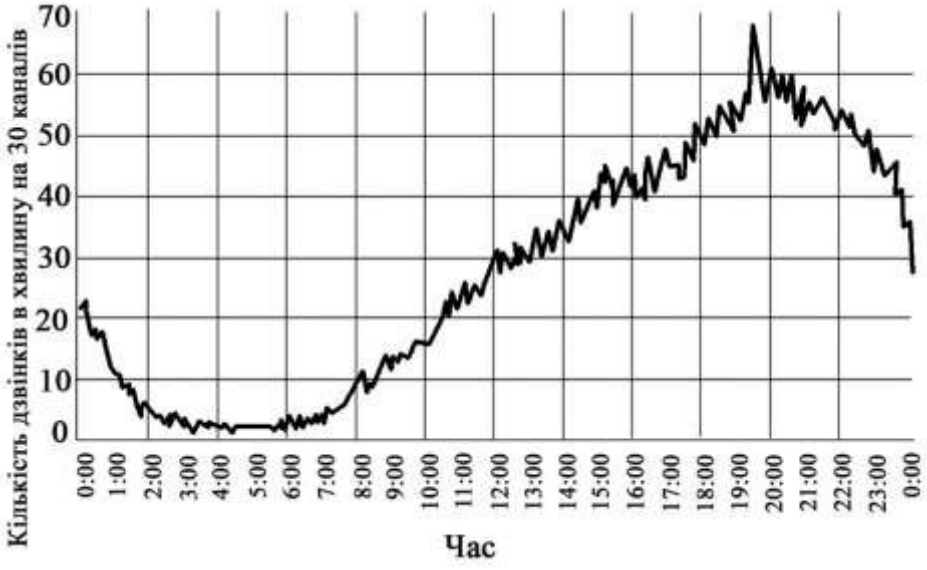

Рисунок 1.6 – Добовий розподіл дзвінків на 30 каналів в хвилину

Реалізація IVR-платформи

Структура меню

Для створення меню голосових додатків виробники зазвичай надають графічні редактори. Для формування сценаріїв обробки дзвінків в основному використовуються блок-схеми.

IVR, керований тоновим набором є ієрархічним додатком. У додатках, що використовують системи ASR (Automatic Speech Recognition) і керуються голосом, меню може бути "плоским", тобто абонентові не потрібно послідовно здійснювати тоновий набір, щоб дістатися до потрібного пункту меню, а досить сказати, що він хоче, і IVR за ключовими словами зрозуміє його. За основу для створення меню необхідно взяти відкритий засіб, що має ієрархічну структуру. На сьогоднішній день кращий вибір – стандарт XML, який володіє наступними можливостями:

– створення ієрархічного меню природним та інтуїтивно зрозумілим способом;

– застосування існуючих парсерів для обходу структури меню;

– використання наявних розробок зі створення та редагування ієрархічних структур;

– зберігання меню в текстовому вигляді, що дозволяє здійснювати доведення IVR у замовника, де необхідне програмне оточення звичайно відсутнє.

Бізнес-логіка

Для отримання необхідної інформації IVR може звертатися до різних джерел даних, використовуючи різноманітні протоколи та мови доступу: SQL, HTTP, TCP, протокол мережевого адміністрування – SNMP (Simple Network Management Protocol), протокол електронної пошти – SMTP (Simple Mail Transfer Protocol), протокол для доступу до SMS / USSD центрів – SMPP (Short Message Peer-to-Peer). Отже, для виконання цього завдання IVRсистема повинна надати гнучкий механізм.

Більшість виробників йдуть по шляху створення власних мов для підтримки доступу до зовнішніх систем. Це рішення виправдовує себе на початковому етапі, але надалі обертається необхідністю підтримки всього синтаксису мови програмування високого рівня, надання API для всіх популярних протоколів, що, у свою чергу, призводить до залучення значних людських і часових ресурсів для підтримки в актуальному стані даної підсистеми. Інтерпретатор мови повинен бути надійним, продуктивним і простим у використанні. Всі ці вимоги роблять завдання по створенню власної мови надзвичайно трудомістким.

Щоб уникнути проблем необхідно інтегрувати у платформу одну з відкритих мов програмування. Прийнятний варіант - використання мови Perl, який незамінний при роботі зі складними структурами текстових даних (наприклад, XML і HTML).

Perl включає бібліотеки для підтримки всіх розповсюджених протоколів і джерел даних. Можливість інтеграції з програмами на C++, дозволяє використовувати C++ для розробки самої IVR-платформи.

Даний мова є інтерпретатором, запускається з командного рядка, що дозволяє здійснювати доведення логіки IVR у замовника без установки додаткового програмного забезпечення. Відкритий код дає можливість вносити необхідні зміни в інтерпретатор Perl самому, а не чекати підтримки від розробників мови.

Багатоплатформність

IVR підтримує багатоплатформність (працює на різних операційних системах). З цією метою при розробці платформи необхідно дотримуватися ANSI стандарту C++ і не використовувати функції, залежні від конкретної операційної системи. Для реалізації системних викликів застосовуються багатоплатформні бібліотеки.

У наш час, побудовою IVR систем займаються спеціалізовані компанії, кожна з яких має свій підхід, заснований на конкретному програмному та технічному забезпеченні[9].

1.7 Необхідність забезпечення інформаційної безпеки IVR-систем

Цінність систем голосового самообслуговування чудово усвідомлюють не тільки власники контакт-центрів, але й клієнти. Як свідчать результати досліджень, проведених на замовлення Genesys компанією Gene Blackley в 14 країнах Європи, 74% користувачів вважають системи IVR ефективною альтернативою цілодобової телефонної підтримки. Приблизно половина користувачів (52%) готова припинити спілкування з організацією, яка не має задовільно функціонуючої системи IVR.[10] Виходячи с таких показників можна вважати, що впровадження IVR-системи в більшості випадків покращить ставлення клієнта, за рахунок якісного обслуговування, а разом із цим забезпечить процвітання компанії.

Але організації що починають використовувати IVR-системи, дуже часто не звертають увагу на конфіденційність, цілісність та доступність інформації що циркулює в системі, або взагалі вважають що забезпечення інформаційної безпеки непотрібно і до того ж вимагає вкладання певних коштів. Результатами такого відношення може бути, як втрата або розповсюдження баз даних організації, відмова системи в цілому, а як наслідок втрата довіри клієнтів.

У розвинених країнах, де центри обробки викликів вже набули широкого поширення, випадки злому Call/контакт-центрів, IVR-систем – не рідкість, хоча ці інциденти зазвичай замовчуються. Втім, іноді випадки крадіжки даних просочуються в пресу. Серед останніх прикладів злом бази даних компанії Seisint, коли була вкрадена інформація про 32 тисячі фізичних осіб, яка містила імена, адреси, номери соціального страхування і водійських прав. Приблизно в цей же час компанія Retail Ventures оголосила про розкрадання частини бази даних, в яку входили номери кредитних карт та інша інформація фінансового характеру.

1.8 Висновок

IVR – системи дозволяють автоматизувати обслуговування клієнтів. Їх використовують банки, мобільні оператори, сервісні центри та інші установи для ефективного обслуговування клієнтів, також IVR-системи використовують для автоматичного сповіщення, телефонного голосування, як довідкові служби і цілодобові центри обслуговування клієнтів. Інтерактивне голосове меню може бути як статичним, так і динамічним в залежності від потреб компанії що його використовує. IVR-система являє собою початкову точку для клієнта при роботі з Call/контакт – центром компанії. Так як Call/контакт – центри можуть бути, як власними, так і аутсорсиногвими, то теж саме можна казати про і IVR – систему.

Так як IVR–система являє собою засіб взаємодії з клієнтом, важливо що б дана система була якісно налаштована, працювала без збоїв та інформація, що в ній циркулює, була надійно захищена, це дозволить зберігати довіру клієнтів, а компанії економити кошти, за рахунок автоматизації процесу, та надавати високий рівень обслуговування клієнтам.

РОЗДІЛ 2. СИНТЕЗ ПІДСИСТЕМИ ЗАХИСТУ IVR СИСТЕМИ

2.1 Інноваційний ризик

Використання інноваційних ідей та нових технологій завжди обтяжене ризиком, а спроби уникнути інновацій здатні зупинити прогрес розвитку компаній. Розробка і впровадження IVR-системи компанії безпосередньо пов’язано з інноваційним ризиком.

В даному випадку інноваційний ризик – це міра можливих збитків, які можуть виникнути у разі вкладення коштів компанії в побудову схеми роботи і впровадження IVR-системи, яка може бути не відразу сприйнята клієнтом компанії, або взагалі бути.

Здобуття додаткової інформації у відповідній сфері є одним з важливих способів щодо зниження інноваційного ризику. Під час використання неточних економічних даних виникає питання щодо доцільності їх уточнення. Що стосується планованих заходів, особливо інноваційних проектів (в нашому випадку, впровадження IVR-системи), то постає питання: чи необхідно терміново почати їх впровадження, чи є сенс провести ще якийсь додатковий експеримент для уточнення економічних показників. З одного боку, додатковий експеримент дозволив би знизити економічний ризик, що обтяжує певний інноваційний проект, зменшити можливі збитки. Але, з іншого боку, експеримент, в свою чергу, пов’язаний з певними затратами та збитками, і якщо впровадження інноваційного проекту відкладається, то економічні збитки збільшуються. Вони особливо великі у разі проведення довгострокового експерименту. У цьому випадку впровадження заходів і одержуваний в результаті цього економічний ефект відсуваються. Прикладом може бути працюючий Call центр, не маючий IVR-системи. Час витрачений на виявлення необхідності впровадження IVR-системи, тягне за собою витрати, пов’язані з заробітною платою операторів, орендою приміщення, платою за телефонні дзвінки.

Отже, для оцінки доцільності добування додаткової інформації необхідно порівняти економічні результати обох варіантів.

Природно, що коли б у менеджера була більш повна інформація, він міг би зробити кращий прогноз й знизити ступінь ризику.

2.2 WideCoup Visual IVR

WideCoup Visual IVR – рішення, що дозволяє створювати інтерактивне голосове меню(IVR – interactive voice response) і вести облік не лише статистики вступу і проходження дзвінків по гілках голосового меню, але і по піковому завантаженні каналів. Дзвінки з телефонної мережі загального користування в систему IVR поступають за допомогою цифрових потоків ISDN PRI через АТС, що забезпечує транзитні з'єднання (рисунок 2.1). Це рішення містить не лише засоби, що забезпечують безпосередню роботу голосового меню але і й інтуїтивно-зрозумілу утиліту для управління ним з будь-якої робочої станції під управлінням ОС Windows. Статистика роботи IVR доступна у вигляді інтерактивних Веб-сторінок системи звітності WideCoup Visual IVR Reports і не вимагає установки клієнтського програмного забезпечення.

2.2.1 Архітектура WideCoup Visual IVR

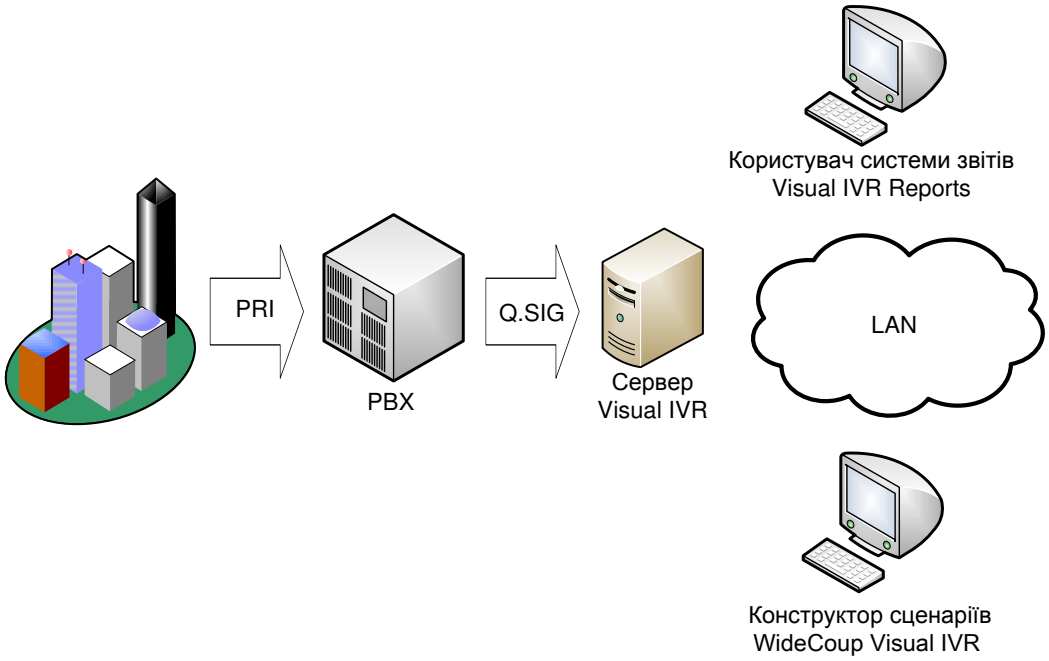

Рисунок 2.1 – Архітектура рішення WideCoup Visual IVR

PRI

Інтерфейс первинного рівня (англ. Primary Rate Interface, PRI) – стандартний інтерфейс мережі ISDN, що визначає дисципліну підключення станцій ISDN до широкосмугових магістралей, що зв'язують місцеві і центральні АТС або мережеві комутатори.

PBX

(Private Branch Exchange (приватна (відомча) АТС)) АТС, обслуговуюча, як правило, державні або приватні організації і розташована в будівлях, в яких працює користувач.

QSIG

Протокол сигналізації, прийнятий організацією ETSI, що базується на ISDN, що забезпечує спільну роботу будь-яких цифрових АТС, при використанні для їх з'єднання інтерфейсу PRI. Він дозволяє використовувати можливості, що працюють тільки на одній міні АТС (парковка виклику, зворотний виклик, і т. д.), для цілої розподіленої мережі з безлічі офісних АТС.

ISDN

Цифрова мережа з інтеграцією обслуговування (англ. Integrated Services Digital Network, ISDN). Дозволяє поєднати послуги телефонного зв'язку і обміну даними.

CDR

Детальний запис про виклик(англ. Call Detail Record, CDR) в телекомунікаційній сфері – файл, що містить інформацію про роботу устаткування, таку, як ідентифікатор джерела дзвінка, ідентифікатор призначення, тривалість і вартість кожного дзвінка, загальний час роботи за період, що тарифікується, час, що залишився, і списана за цей період сума. Формат CDR визначається телекомунікаційним оператором або програмою.

Рішення WideCoup Visual IVR складається з наступних основних модулів:

− сервера IVR, приймаючого телефонні дзвінки і що безпосередньо реалізує інтерактивне голосове меню, а також формує первинні дані для звітів

(CDR);

− системи звітності WideCoup Visual IVR Reports (встановлюються на той самий сервер);

− конструктора сценаріїв голосового меню WideCoup Visual IVR, який забезпечує відображення, редагування і застосування голосового меню на сервері а також зміну конфігураційних файлів системи звітності. Конструктор сценаріїв встановлюється на робочі станції адміністраторів голосового меню.

Сервер IVR знаходиться під управлінням ОС Debian GNU/Linux 4.0 і містить PRI-плату Digium стандарту PCI або PCI – Express, яка забезпечує той, прийом телефонних дзвінків цифровими каналам ISDN PRI. Крім того, на сервер IVR встановлюється додаткове програмне забезпечення, яке забезпечує роботу усього рішення в цілому (рис. 2.2):

− IP-PBX Asterisk – основна частина системи, забезпечує отримання телефонних дзвінків і функціонування голосового меню;

− СУБД MySQL для зберігання даних CDR і довідників системи звітності WideCoup Visual IVR Reports;

− інтерпретатор PHP – забезпечує роботу системи звітності WideCoup Visual IVR Reports

− сервер Веб-публикаций Apache – забезпечує функціонування інтерактивних Веб-сторінок системи звітності WideCoup Visual IVR Reports;

− ftp-сервер proftpd – забезпечує прийом/передачу конфігураційних файлів IP-PBX Asterisk і звукових файлів для роботи голосового меню.

При створенні голосового меню за допомогою конструктора сценаріїв WideCoup Visual IVR в спеціальній директорії цього програмного забезпечення створюються наступні файли:

− сценарій голосового меню у вигляді конфігураційних файлів IP-PBX Asterisk;

− голосові файли для програвання в голосовому меню;

− xml-файли, що містять зв'язок між конфігурацією IP-PBX Asterisk і та назви пунктів голосового меню (потрібні також для роботи системи звітності).

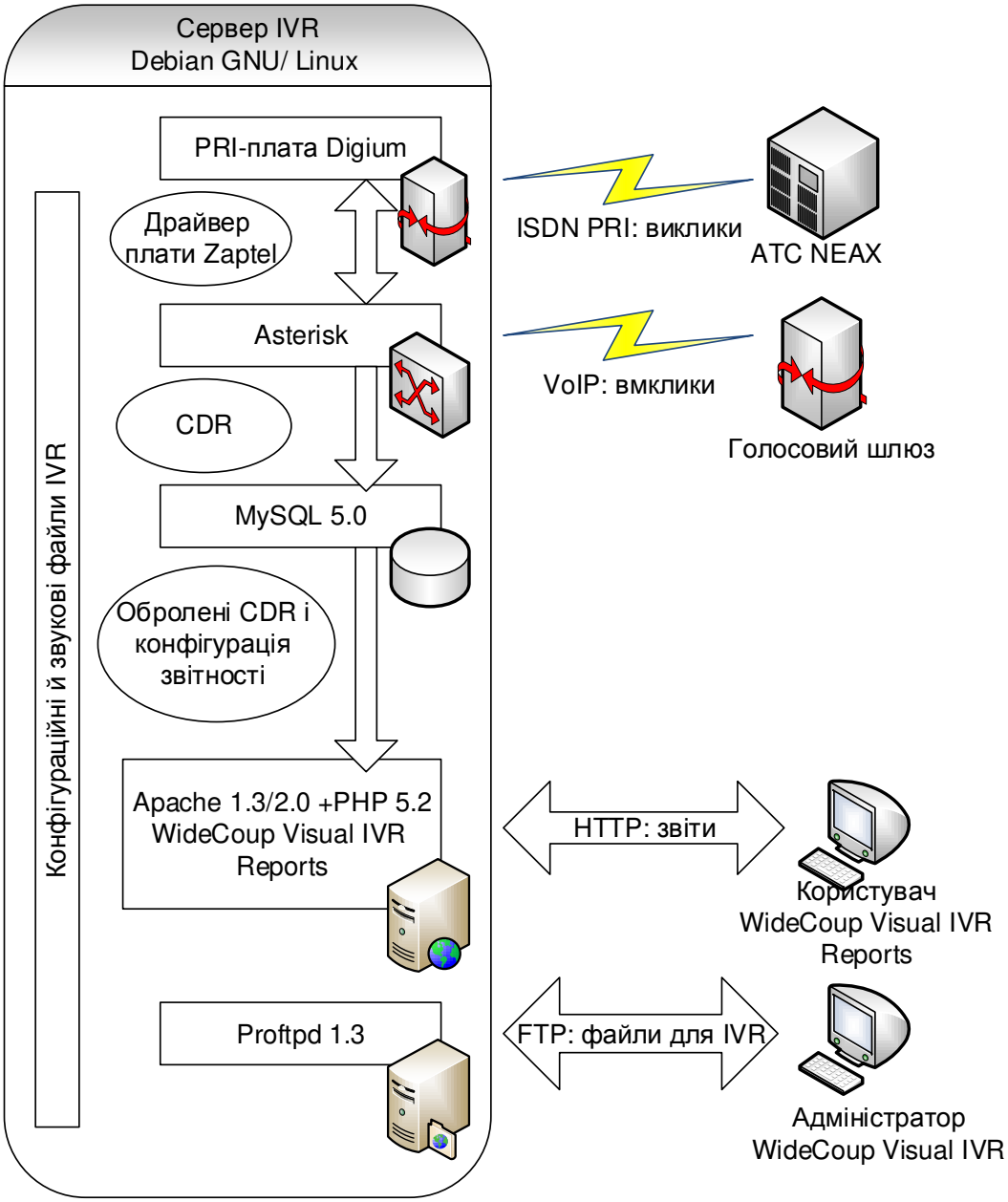

Рисунок 2.2 – Архітектура і схема взаємодії сервера IVR

Для внесення змін до поточної конфігурації системи IVR конструктор сценаріїв WideCoup Visual IVR передає усі вищезгадані файли по протоколу FTP на сервер IVR і дає команду IP-PBX Asterisk на застосування нової конфігурації.

Для отримання поточної конфігурації системи IVR конструктор сценаріїв WideCoup Visual IVR викачує по протоколу FTP необхідні для роботи файли і генерує поточний сценарій голосового меню з можливістю прослуховування

голосових файлів і внесення необхідних змін.

Система звітності WideCoup Visual IVR Reports, використовуючи конфігураційні xml-файли сценарію і CDR дані IP-PBX Asterisk, в яких відображені переходи користувачів по гілкам сценарію голосового меню, формує звіти, що показують інтерес абонентів по відношенню до різних пунктів голосового меню, шляхів проходження дзвінків у рамках усього сценарію і піковому завантаженню каналів за вказані періоди часу.

2.2.2 Системні вимоги

2.2.2.1 Сервер IVR

Системні вимоги апаратної частини рішення WideCoup Visual IVR залежить від фактичного телефонного навантаження на на сервер IVR. Рекомендовані вимоги до сервера IVR для 30 каналів (один ISDN PRI) при середньому навантаженні (до 10 годин на добу):

- одно процесорна платформа (тактова частота процесора не нижче 2,4 ГГц);
- не менше 2 Гб оперативної пам'яті;
- два HDD, об’ємом не менше 250 Гб (для організації RAID-1);
- наявність слота PCI-Express для установки плати Digium PRI.

Системні вимоги в частині програмного забезпечення сервера IVR складають:

- ОС Debian GNU/ Linux останнього стабільного релізу;
- IP-PBX Asterisk серії з 1.4;
- СУБД MySQL серії з 5;
- ftp-сервер proftpd, стабільна версія не нижче 1.3.0.

2.2.2.2 Система звітності WideCoup Visual IVR Reports

Система звітності WideCoup Visual IVR Reports розгортається зазвичай на самому сервері IVR і додатково вимагає:

- інтерпретатор PHP серії 5, стабільна версія не нижче 5.2.0;
- сервер Веб-публикаций Apache серії 1.3/2.0.

Установка усіх вищеописаних модулів припускає установку необхідних для їх роботи пакетів, що входять до складу ОС Debian GNU/ Linux.

Для роботи користувачів з системою звітності WideCoup Visual IVR Reports рекомендується браузер Microsoft Internet Explorer 7 або вище.

2.2.2.3 Конструктор сценаріїв WideCoup Visual IVR

Робоча станція під управлінням ОС Windows 7/8/10. Для зручності роботи бажана наявність звукової карти і аудіосистеми для прослуховування голосових файлів.

2.3 Аналіз загроз

Всі джерела загроз безпеки інформації, яка має комерційну цінність, або підлягає захисту в силу закону і циркулює в CRM-системі, а саме в її головному модулі IVR, можна розділити на три основні групи:

I Загрози, обумовлені діями суб'єкта (антропогенні загрози).

II Загрози, обумовлені технічними засобами (техногенні загрози).

III Загрози, обумовлені стихійними джерелами.

Нижче приведений список загроз, що мають найвищий рівень критичності для системи, і підлягають захисту в першу чергу.

I Антропогенного характеру:

1) Крадіжка інформації (читання і несанкціоноване копіювання), засобів доступу (ключі, паролі, ключова документація тощо) та технічних засобів (вінчестерів, ноутбуків, системних блоків);

2) Підміна (модифікація) паролів та ключів доступу;

3) Знищення носіїв інформації чи самої інформації (файлів, даних), програмного забезпечення (ОС, СУБД, прикладного ПЗ);

4) Порушення пропускної можливості каналів зв’язку та порушення нормальної роботи електроживлення технічних засобів.

5) Помилки при експлуатації ПЗ.

6) Перехоплення інформації при підключенні до каналів передачі інформації та перехоплення інформації (несанкціоноване) за рахунок порушення встановлених правил доступу (злом).

II Техногенного характеру:

1) Порушення працездатності зв'язку і телекомунікацій, старіння носіїв інформації і засобів її обробки;

2) Знищення (руйнування) засобів обробки інформації (стрибки напруги).

III Стихійні лиха:

Знищення (руйнування):

- технічних засобів обробки інформації;
- програмного забезпечення (ОС, БД, прикладного ПО);
- інформації (файлів, даних);
- приміщень.

Далі представлена таблиця, в якій більш детально розглянуто основні загрози IVR системи (таблиця 2.1), де К – конфіденційність, Ц – цілісність, Д – доступність, С – спостереженість.

Таблиця 2.1 – Основні загрози IVR систем та рівень можливих збитків

Дії, обумовлені дією суб'єктів						
Загроза	На що направлена	Що порушує	Рівень критичності	Середній рівень критичності	Зона ризику збитків	Рівень збитків
Крадіжка інформації	база даних організації, статистика звернень, особиста інформація клієнтів	К	4	4	критична	великий
Підміна паролів та ключів доступу	сценарій голосового меню, база даних організації, статистика	К	4	3,5	критична	великий
		Ц	4			

	звернень, особиста інформація клієнтів	Д	3			
		С	3			

Продовження таблиці 2.1

Загроза	На що направлена	Що порушує	Рівень критичності	Середній рівень критичності	Зона ризику збитків	Рівень збитків
Підміна інформації	сценарій голосового меню, статистика звернень	Ц	3	3	критична	великий
		Д	3			
Знищення носіїв інформації чи самої інформації	працездатність системи, сценарій голосового меню, голосові файли, база даних організації, статистика звернень, особиста інформація клієнтів	Ц	4	4	критична	катастрофічний
		Д	4			
		С	4			
Порушення пропускної можливості каналів зв’язку та порушення нормальної роботи електроживлення технічних засобів	працездатність системи, база даних організації, статистика звернень, особиста інформація клієнтів	Ц	3	3	критична	великий
		Д	3			
		С	3			

Продовження таблиці 2.1

Загроза	На що направлена	Що порушує	Рівень критичності	Середній рівень критичності	Зона ризику збитків	Рівень збитків
Помилки при експлуатації ПЗ	працездатність системи, сценарії голосового меню, база даних організації, статистика звернень, особиста інформація клієнтів	К	3	2,25	допусти-ма	середній
		Ц	2			
		Д	2			
		С	2			
Перехопле-ння інформації	база даних організації, статистика звернень, особиста інформація клієнтів	К	4	4	критична	великий
Дії, обумовлені дією технічних засобів						
Порушення працездатності зв'язку і телекомуніка-цій, старіння носіїв інформації і засобів її обробки	працездатність системи, сценарій голосового меню, голосові файли, база даних організації, статистика звернень, особиста інформація клієнтів	Ц	2	2,33	допусти-ма	помірко-ваний
		Д	2			
		С	3			

Продовження таблиці 2.1

Загроза	На що направлена	Що порушує	Рівень критичності	Середній рівень критичності	Зона ризику збитків	Рівень збитків
Знищення (руйнування) засобів обробки інформації (стрибки напруги)	працездатність системи, сценарій голосового меню, голосові файли, база даних організації, статистика звернень, особиста інформація клієнтів	Ц	3	3,5	критична	катастрофічний
		Д	4			
Дії, обумовлені дією стихійних лих						
Знищення (руйнування)	працездатність системи, сценарій голосового меню, голосові файли, база даних організації, статистика звернень, особиста інформація клієнтів	Ц	4	4,66	катастро-фічна	катастрофічний
		Д	5			
		С	5			

2.4 Модель порушника

Для більш детального аналізу загроз IVR-системи розроблена модель порушника.

Таблиця 2.2 – Категорії порушників в IVR системі

Позначення	Визначення категорії	Рівень загрози
Внутрішні		
ПВ1	Технічний персонал який обслуговує приміщення (електрики, сантехніки, прибиральниці), в якому розташована база даних клієнтів IVR системи	1

Продовження таблиці 2.2

Позначення	Визначення категорії	Рівень загрози
ПВ2	Персонал, який обслуговує технічні засоби(інженери, техніки)	2
ПВ3	Користувачі (оператори) програм	3
ПВ4	Співробітники підрозділів, робота яких пов'язана з розробкою і супроводом програмного забезпечення, або інших підрозділів і організацій, які притягуються до таких робіт	4
ПВ5	Адміністратори систем	4
Зовнішні		
ПЗ1	Відвідувачі(запрошені з деякого приводу)	1
ПЗ2	Представники організацій, які взаємодіють з питань технічного забезпечення і експлуатації будівель (енерго, водо, теплопостачання і т.п.)	2
ПЗ3	Висококваліфікований зловмисник	4

Таблиця 2.3 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загрози
П1	Безвідповідальність	2
П2	Самоствердження	2
П3	Корисливий інтерес	5
П4	Професійний обов'язок	5

Таблиця 2.4 – Специфікація моделі порушника за рівнем кваліфікації

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних і потоків запитів до них, має навички відносно користування штатними засобами	1
К2	Володіє високим рівнем знань і практичними навичками роботи з технічними засобами системи і їх обслуговування	2

К3	Володіє високим рівнем знань в області програмування і обчислювальної техніки, проектування і експлуатації IVR-систем	2
К4	Знає структуру, функції і механізми дії заходів захисту інформації в організації відносно IVR-системи а також їх недоліки	3
К5	Знає недоліки механізмів захисту, які вбудовані в системне програмне забезпечення і її не документовані можливості	4
К6	Є розробником програмних і програмно-апаратних засобів захисту або системного програмного забезпечення	5

Таблиця 2.5 – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загрози
М1	Без доступу на контрольовану територію	1
М2	З контрольованою території без доступу в будинки і споруди	1
М3	Усередині приміщень, але без доступу до технічних засобів IVR - системи	2
М4	З робочих місць користувачів(операторів) IVR - системи	3
М5	З доступом в зони даних(серверні бази даних)	3
М6	З доступом в зону управління засобами забезпечення безпеки IVR - системи	4

Оцінка рівня загроз проведена за п’ятибальною шкалою.

З представлених таблиць можна стверджувати, що найбільшу загрозу для IVR системи несуть співробітники які мають до неї безпосередній доступ.

2.5 Експертна оцінка профілю захищеності

Для забезпечення конфіденційності, цілісності і доступності оброблюваної інформації в IVR-системі, згідно з НД ТЗІ 2.5-005-99, був обраний наступний профіль захищеності,

3.КЦД.2 = {КД-2, КА-2, КО-1, КВ-2,
ЦД-1, ЦА-2, ЦО-1, ЦВ-2,
ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

1) Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні

даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

КД-2. Базова довірча конфіденційність

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

НЕОБХІДНІ УМОВИ: НИ-1

2) Адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

КА-2. Мінімальна адміністративна конфіденційність

Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процессу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

НЕОБХІДНІ УМОВИ: НО-1, НИ-1

3) Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КО-1. Повторне використання об'єктів

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в данному об'єкті, повинна стати недосяжною

4) Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

КВ-2. Базова конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності.

Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процессу.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процессу.

НЕОБХІДНІ УМОВИ: НО-1

5) Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦД-1. Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати

множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

НЕОБХІДНІ УМОВИ: НИ-1

6) Адміністративна цілісність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦА-2. Базова адміністративна цілісність

Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів

визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

НЕОБХІДНІ УМОВИ: НО-1, НИ-1

7) Відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

ЦО-1. Обмежений відкат

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

НЕОБХІДНІ УМОВИ: НИ-1

8) Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

ЦВ-2: Базова цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процессу.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процессу

Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

НЕОБХІДНІ УМОВИ: НО-1

9) Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

ДР-1. Квоти

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

НЕОБХІДНІ УМОВИ: НО-1

10) Відновлення після збоїв

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

НЕОБХІДНІ УМОВИ: НО-1

11) Реєстрація

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються.

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до Безпеки.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НЕОБХІДНІ УМОВИ: НИ-1, НО-1

12) Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ .

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ автентифікувати цього користувача з використанням захищеного механізму.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнуванняю

НЕОБХІДНІ УМОВИ: НК-1

13) Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

14) Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної

послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

НО-2. Розподіл обов'язків адміністраторів.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НЕОБХІДНІ УМОВИ: НИ-1

15) Цілісність комплексу засобів захисту

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

16) Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НЕОБХІДНІ УМОВИ: НО-1

17) Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації.

НВ-1: Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації

2.5 Реалізація профілю захищеності

Реалізувати критерії побудованого профілю захищеності для обраної IVR системи, можна за вдяки наступним засобам:

2.5.1 Гриф-Мережа

Комплекс засобів захисту ІзОД, від НСД “Гриф-Мережа” призначений для забезпечення захисту ІзОД, що обробляється в ЛОМ.

Комплекс дозволяє створити на базі ЛОМ спеціалізовану АС для обробки ІзОД і забезпечити захист оброблюваної ІзОД від загроз порушення цілісності, конфіденційності та доступності при реалізації політики адміністративного управління доступом до інформації.

Комплекс «Гриф-Мережа» реалізує наступні функції:

– Ідентифікацію та аутентифікацію користувачів на підставі імені, пароля і персонального електронного ідентифікатора (Touch Memory, Flash Drive або дискети) при завантаженні ОС робочої станції до завантаження будь-яких програмних засобів з дисків, що дозволяє заблокувати використання робочої станції сторонньою особою, а також пізнати конкретного легального користувача і надалі реагувати на запити цього користувача відповідно до його повноважень;

– Блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

– Контроль цілісності і самотестування КСЗ при старті і за запитом адміністратора, що дозволяє забезпечити стійке функціонування КСЗ і не допустити обробку ІзОД у разі порушення його працездатності;

– Розмежування обов'язків користувачів і виділення кількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію захищаються ресурсів, реєстрацію користувачів, призначення прав доступу, обробку протоколів аудиту тощо).

– Розмежування доступу користувачів до обраних каталогів (папок), розміщеним на робочих станціях і файлових серверах ЛВС, що дозволяє організувати одночасну спільну роботу декількох користувачів ЛОМ, що мають різні службові обов'язки і права з доступу до ІзОД;

– Управління потоками інформації і блокування потоків інформації, що призводять до зниження рівня її конфіденційності;

– Контроль за виведенням інформації на друк;

– Контроль за експортом / імпортом інформації на змінні носії;

– Гарантоване видалення інформації шляхом затирання вмісту файлів, що містять ІзОД, при їх видаленні;

– Розмежування доступу прикладних програм до обраних каталогів і файлів що в них знаходяться, що дозволяє забезпечити захист ІзОД від випадкового видалення, модифікації і дотримати технологію її обробки;

– Контроль цілісності прикладного ПЗ та ПЗ КСЗ, а також блокування завантаження програм, цілісність яких порушена, що дозволяє забезпечити захист від вірусів і дотримання технології обробки ІзОД;

– Контроль за використанням користувачами дискового простору файлових серверів (квоти), що виключає можливість блокування одним з користувачів можливості роботи інших;

– Відновлення функціонування КСЗ після збоїв, що гарантує доступність інформації з забезпеченням дотримання правил доступу до неї;

– Безперервну реєстрацію, аналіз і обробку подій (входу користувачів в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з ІзОД, виведення на друк і т.п.) в спеціальних протоколах аудиту, що дозволяє адміністраторам контролювати доступ до ІзОД, стежити за тим, як використовується КСЗ, а також правильно його конфігурувати;

– Негайне сповіщення адміністратора безпеки про всі виявлені порушення встановлених правил розмежування доступу (ПРД);

– Ведення архіву зареєстрованих даних і даних аудиту.

До складу комплексу «Гриф-Мережа» входять:

– Засоби розмежування доступу і реєстрації даних аудиту, що встановлюються на робочих станціях і файлових серверах ЛОМ;

– АРМ адміністратора засобів захисту. Основні функції: реєстрація користувачів, вироблення даних ідентифікації і аутентифікації із збереженням їх на ідентифікаторах; реєстрація ресурсів, що захищаються; управління розмежуванням доступу користувачів до обраних каталогів; контроль цілісності і самотестування КСЗ за запитом адміністратора; управління розмежуванням доступу прикладних програм до обраних каталогів; управління квотами

користувачів; установка контролю програмного забезпечення (заборона запуску незареєстрованих програм);

– АРМ адміністратора безпеки. Основні функції: настройка і управління параметрами аудиту захищених ресурсів; управління параметрами оповіщення та прийом повідомлень про критичних для безпеки події в режимі реального часу; можливість перегляду, аналізу й обробки протоколів аудиту; робота з архівом даних аудиту.

Розробка виконана у відповідності з вимогами до рівня гарантій Г-4[14].

Реалізує наступні критерії профілю захищеності: КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-5, НИ-3, НК-1, НО-2, НЦ-2, НТ-2**.**

2.5.2 IBM Tivoli Continuous Data Protection

IBM Tivoli Continuous Data Protection – це гарантоване відновлення даних за рахунок безперервного автоматичного створення, відстеження та зберігання точок відновлення. Реалізується за допомогою розгортання другорядного сервера для зберігання даних.

Особливості:

– Спрощене керування системою зберігання дозволяє знизити трудовитрати фахівців в області IT і кінцевих користувачів.

– Безперервний захист даних забезпечує їх збереження при вірусних атаках і апаратних збоїв.

– Усунення прогалин в процесах резервного копіювання даних.

– Оптимізація процесів інтеграції програм, призначених для захисту даних робочої мережі і підприємства.

– Оптимізація пропускної здатності та процесів передачі даних у мережі.

– Безперервній захист версій файлів, що дозволяє вибирати потрібну точку відновлення.

– Можливість локального запису захищених даних в автономному режимі (без підключення до мережі) у разі вірусної атаки, аварійного збою, логічної помилки або помилки користувача.

– Можливість збереження даних на пристроях резервного копіювання різного типу (жорсткі диски, мережеві пристрої зберігання (NAS), пристрої USB, логічні розділи, логічні пристрої SAN).

– Можливість створення точок відновлення з високим ступенем дроблення і змінності.

– У разі втрати або пошкодження даних CDP дозволяє відновити будь-яку зі збережених копій вихідного файлу, навіть якщо помилка виникла за кілька днів до виявлення наслідків. CDP for Files забезпечує можливість швидкого відновлення файлу в початковий стан - для цього може знадобитися від декількох секунд до декількох хвилин.

– Просте архівування: збереження файлів із захистом від несанкціонованого втручання.

– Зберігання файлів даних протягом заданого періоду часу.

– Простота налаштування – зручний користувальницький інтерфейс.

IBM Tivoli Continuous Data Protection (CDP) for Files V3.1 забезпечує збереження даних завдяки безперервному захисту найбільш важливих файлів користувача, включаючи документи, над якими ведеться активна робота. Це дозволяє зменшити або усунути прогалини в процесах резервного копіювання даних і забезпечити ефективну та дієву захист даних у кінцевих точках. Це ПЗ допомагає здійснювати відновлення даних після збоїв, викликаних вірусними атаками, пошкодження даних і помилками користувачів.

Tivoli CDP for Files є альтернативою традиційним підходам до резервного копіювання кінцевих точок. Це ПЗ орієнтовано на використання доступної технології використання жорстких дисків як сховище резервних копій даних. У момент збереження файлу Tivoli CDP for Files створює копії цього файлу для відправки в різні місця розташування або пункти призначення. Таким чином

здійснюється захист файлів. Нижче наведено список різних пунктів призначення:

– Локальний кеш – локальний диск, що забезпечує захист даних, навіть коли комп'ютер не підключений до мережі.

– Мережева файлова система - для захисту даних за межами системи на платформах зберігання даних NAS, наприклад, IBM серії N

– Web-адреса – функція реплікації на Web-сайти, призначена для постачальників послуг Інтернету.

– Tivoli Storage Manager – середовища, що використовують Tivoli Storage Manager.

– Tivoli Storage Manager Express[15].

2.5.3 Міжмережевий екран Cisco ASA 5500

Пристрій адаптиваного захисту Cisco ASA 5500 Series представляє собою просте в розгортанні рішення, що інтегрує сервіси міжмережевого екрану, безпеки уніфікованих комунікацій (передача голосових і відеоданих), VPN з підтримкою SSL і IPsec, системи запобігання вторгнень (IPS) і безпеки контенту в гнучке сімейство модульних продуктів. Пристрій Cisco ASA 5500 Series надає інтелектуальний захист від загроз і послуги безпечних комунікацій, які зупиняють поширення атак перш, ніж вони зможуть чинити негативний вплив на цілісність бізнесу. Cisco ASA 5500 Series призначений для захисту мереж усіх масштабів і дозволяє організаціям скоротити загальні витрати на розгортання та експлуатацію, одночасно забезпечуючи комплексну багаторівневу безпеку.

Cisco ASA 5580 являє собою високопродуктивну платформу безпеки, яка підходить для роботи в якості масштабованого міжмережевого екрану з пропускною спроможністю до 20 Гбіт/с і в якості концентратора віддаленого доступу в мережах SSL / IPSec VPN на 10 тисяч користувачів.

Cisco ASA 5580 призначено для захисту мультимедійних транзакційних додатків, які чутливі до затримок і працюють в корпоративних центрах обробки даних та інтернет-шлюзах. Це рішення має кращу на ринку пропускною здатністю, найвищою в галузі швидкістю з'єднань, широким розмаїттям підтримуваних конфігурацій і дуже низькою латентністю. У результаті Cisco ASA 5580 відмінно підходить для захисту організацій, що використовують найбільш ресурсомісткі програми для передачі голосу, відео і даних, резервування інформації, наукових і фінансових операцій.

Данне рішення дозволить забезпечити належний рівень безпеки як IVR – системи, так і всього Call/контакт – центру в цілому при роботі з мережою Інтернет, не впливаючи на швидкість роботи системи[16].

2.6 Матриця доступу для IVR-системи

Враховуючи інформацію яка може циркулювати в IVR-системі, та коло співробітників які можуть мати до неї доступ, побудована матриця доступу, що описує які дії по відношенню до інформації дозволені тим чи іншим користувачам

Таблиця 2.6 – Матриця доступу

	Оператор	Адміністратор IVR-системи	Користувач системи звітів IVR-системи	Адміністратор мережі	Адміністратор інформаційної безпеки
Параметри загальносистемних налаштувань	-	R, W, D	-	R, W, D	R, W, D
Інформація про групи користувачів	-	-	-	R, W, D	R, W, D
Інформація про клієнтів	W, R	-	-	-	R
Глобальна адресна книга	W, R	R, W, D	-	-	-
Умови маршрутизації викликів	-	R, W, D	-	-	R, W, D
Списки розсилки оголошень	-	R, W, D	-	-	-

Сценарії голосового меню	-	R, W, D	R	-	R
Статистика для звітності	-	R	R	R	R
Голосові файли	-	R, W, D	-	-	R
Конфіденційна інформація клієнта	-	-	-	-	R, W, D

R – можливість зчитувати файл

W – можливість змінювати/дописувати в файл

D – можливість видаляти файл

2.7 Оплата послу за допомогою VISA і MasterCard карток

Останнім часом широкого поширення набула оплата послуг за допомогою VISA и MasterCard карток в системі інтерактивного голосового меню. Прикладом може бути ситуація, коли клієнт зателефонувавши в службу підтримки свого мобільного оператора, користуючись підказками IVR–системи, обирає необхідну послугу, вводить номер кредитної карти та її CVV2/CVC2 код, для оплати обраної послуги. Оплати можуть бути як разовими, так і, наприклад, щомісячними, тобто система буде автоматично знімати кошти з рахунку клієнта для оплати послуги. Такий процес потребує високого рівня інформаційної безпеки IVR–системи, тому що клієнт надає компанії конфіденційну інформацію, яка в свою чергу повинна бути надійно захищена.

По перше, надаючи такі послуги, IVR–система повинна бути власністю компанії, тобто користування послугами аутсорсингових компаній неприпустимо, тому що в такому випадку не можливо здійснювати повний контроль доступ до конфіденційної інформації клієнта. Слід зауважити, що використання IVR–системи, яка була розроблена, впроваджена і обслуговується компанією–власником є найбільш прийнятним варіантом з точки зору інформаційної безпеки. Тобто використання готових технічно-програмних рішень, які обслуговуються компанією–розробником збільшує можливість неконтрольованого витоку конфіденційної інформації.

По друге, доступ до конфіденційної інформації повинен бути обмежений. Тобто потрібне розмежування доступу на рівні користувачів системи. Рекомендуємі параметри наведені в матриці доступу (таблиця 2.6). Природно, що звуження кола співробітників що мають доступ до інформації, зменшує ризик її розповсюдження.

По третє, конфіденційна інформація має зберігатися в шифрованому вигляді, ключ для дешифрування даних має бути тільки в співробітника відділу інформаційної безпеки. Дані мають розшифровуватись тільки в оперативній пам'яті під час безпосередньої роботи з системою.

Окрім програмно–технічних заходів по захисту конфіденційної інформації, мають бути розроблені інструкції з організаційного захисту інформації. Звернення клієнтів, що стосуються вводу або керування конфіденційною інформацією не повинні проходити за допомогою технології розпізнавання мови. Це обумовлено тим, що клієнт може не мати змоги продиктувати інформації вголос і крім того тоновий набір більш надійний для вводу цифр, з яких звичайно складається номер рахунку/кредитної картки, або пароль для входу в систему. Якщо пароль був введений невірно три рази поспіль, виклик повинен автоматично переадресовуватись до співробітника за дану послугу.

2.8 Рекомендації щодо захисту конфіденційної інформації в IVR системах

На думку вітчизняних і зарубіжних експертів у галузі інформаційної безпеки, багато замовників і постачальники таких бізнес-рішень як IVR системи не приділяють належної уваги захисту інформації, причому основна загроза її безпеці виходить від недобросовісних співробітників.

Погана захищеність IVR систем частково пояснюється прагненням їх власників мінімізувати витрати на обслуговування викликів, що призводить до зниження надійності системи та пов'язаної з нею інфраструктури.

Для якісного захисту інформації в IVR системі необхідно забезпечувати не лише її власну інформаційну безпеку, але й захист всієї пов’язаної з нею інфраструктури. Наприклад, за словами користувачів обладнання Cisco Systems

застосовувати якісь додаткові рішення по захисту інформації не обов'язково - це завдання можна вирішити в рамках вже існуючих елементів, в які вбудовані спеціальні програмні модулі. Мова йде про такі складові як CallManager, ICM, IP-телефони, програми та інше.

Приміром, на CallManager встановлено спеціальне ПЗ – Cisco Security Agent, яке забезпечує захист цього пристрою від різного роду характерних атак, а також запобігає витоку інформації через USB і інші периферійні пристрої (CD / DVD-приводи, слоти PCMCIA і т.п.). Посилити надійність рішень допомагає додаткове використання поширених в Україні антивірусних програм. Корисним може виявитися також застосування міжмережевих екранів і спеціальних систем запобігання атакам.

Можна сказати, що при правильній організації взаємодії з базами даних і іншими додатками IVR меню не вносить додаткової уразливості в інформаційну систему. А основними джерелами загрози її безпеки можна вважати програмне забезпечення для роботи з базами даних, оскільки ці програми використовують у своїй роботі аутентифікаційну інформацію. Потенційна небезпека міститися в проміжному ПЗ в якому може затримуватись інформація з CRM системи. Найбільш високу небезпеку складає несанкціоноване і неконтрольоване поширення конфіденційної інформації про клієнтів.

При аутсорсинговому IVR меню необхідно забезпечувати збереження даних як про клієнтів компанії-замовника, так і про характеристики викликів, обслужених системою. Ризик витоку інформації пропорційний кількості співробітників, які мають до неї доступ, тому разом із зменшенням кількості таких осіб буде знижуватися і вірогідність цього витоку.

Для вирішення питань інформаційної безпеки в IVR меню слід використовувати інтеграцію з системою безпеки операційної системи, сертифіковані криптопровайдери для шифрування конфіденційної інформації в базах даних. Ключі розміщувати на відчужуваних носіях (смарт-карти, токени і т.д.); при підключенні клієнтських додатків до баз даних використовувати

захищені з'єднання (SSL). Фіксувати ролі користувачів у системі та повноваження цих ролей, записувати всі дії персоналу для можливості подальшого аудиту цих дій.

Слід сказати, що забезпечити безпеку може тільки комплексний підхід. Тому забезпечення безпеки в системі IVR можна розділити на три категорії: мережева, інформаційна та організаційна.

Для забезпечення мережної безпеки необхідно розмежовувати права доступу на технічному рівні (канали зв'язку, телефонна станція, системи розподілу дзвінків, допоміжні сервери). Інформаційна безпека досягається розмежуванням доступу до програмного забезпечення і даним що в них розміщуються. Операторів слід обмежити тільки тією інформацією, яка їм необхідна при роботі з дзвінками; супервізори повинні мати доступ до статистичних даних, що дозволяє виконувати контроль показників результативності за проектом у своїй групі, а менеджери – до тієї частини інформації, яка визначається взаємодією з замовником.

У поняття «організаційна безпека» включається забезпечення безпеки на рівні «людського фактору». Її реалізація забезпечується за допомогою контролю виконання посадових інструкцій персоналом. Зокрема, сюди включається використання апаратних засобів контролю за діями персоналу за проектом, регламент складання та зберігання документів за проектом, внутрішній аудит безпеки IVR системи та незалежний аудит. Необхідно також встановити персональну відповідальність кожного співробітника, закріплену на юридичному рівні.

Саме організаційна складова є основною в запобіганні витоку інформації з IVR системи. Клієнтські бази даних можуть бути захищені настільки, що несанкціонований доступ до них обійдеться значно дорожче, ніж утримання самої інформації. У більшості випадків витік інформації відбувається з вини співробітників, які мають до неї доступ. Особливо це стосується тих випадків, в яких при створенні IVR системи, користуються послугами сторонніх компаній, для створення власних ресурсів(сервер баз даних, FTP-сервер і т.д.), оскільки

компанія має істотно менший контроль над співробітниками чужої компанії. В цьому випадку, передачу компанією конфіденційної інформації необхідно закріпити офіційним договором. Слід зауважити, що загроза витоку інформації буде існувати до тих пір, поки з нею продовжують працювати сторонні особи.

Що стосується зовнішніх загроз, то їх можна вважати менш актуальними до тих пір, поки для IVR системи виконуються стандартні заходи забезпечення інформаційної безпеки мережі та інформаційних ресурсів. Інформаційна безпека в IVR системі забезпечується, в першу чергу, ефективним управлінням самої системи і тільки потім - технологіями.

Але не можна обмежуватися тільки розмежуванням прав доступу до інформації і програмного забезпечення, необхідно також забезпечувати фізичну безпеку, наприклад захист робочих станцій управління системою, захист серверів. Крім того, для мінімізації ризиків, пов'язаних з інформаційною безпекою CRM-рішень, системні інтегратори нерідко пропонують складене рішення від двох виробників, наприклад Oracle Interaction Center (на базі Oracle E-Business Suite) і Cisco IPCC або Avaya AIC/CCE.

Інформаційну безпеку IVR системи слід розглядати на двох рівнях. По-перше, необхідно оцінювати можливість несанкціонованого доступу до локальної мережі, в яку включені функціональні сервери і бази даних. По-друге, слід чітко контролювати компетентність і сумлінність персоналу, який забезпечує роботу IVR системи, що найчастіше є більш складною і важливою задачею.

2.9 Висновок

В результаті проведеного аналізу структури IVR–системи, були розглянуті основні загрози для даного бізнес рішення. Побудована модель порушника, аналізуючи яку, можна зробити висновок, що найбільшу загрозу для IVR – системи являє собою співробітник компанії.

Були запропоновані засоби реалізації обраного профілю захищеності, що враховує особливості інтерактивного голосового сервісу. Побудована матриця доступу співробітників до IVR–системи, дозволить зменшити можливість

неконтрольованого витоку інформації. Був розглянутий спосіб оплати послуг компанії за допомогою VISA та MasterCard карток в IVR-системах, та надані рекомендації щодо захисту інформації клієнта при проходженні таких операцій. Також були надані загальні рекомендації, організаційного характеру щодо захисту конфіденційної інформації в інтерактивних голосових системах.

Запропоновані методи підвищення інформаційної безпеки можуть використовуватися не лише для конкретної IVR–системи, що була розглянута в дипломній роботі, а й для інших систем, які були розроблені і обслуговуються компанією-власником. Приведені методи допоможуть підвищити рівень інформаційної безпеки не тільки компаніям, що тільки починають використовувати інтерактивні голосові служби але й компаніям, що вже давно використовують дане бізнес рішення.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є економічне обґрунтування підвищення інформаційної безпеки інтерактивної голосової служби шляхом визначення:

– капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;

– річного економічного ефекту;

– показників економічної ефективності підвищення інформаційної безпеки інтерактивної голосової служби.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, $К_{пр}$=5000 грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

Системою інтерактивної голосової взаємодії, в якій користувач може отримати доступ до інформації, яка його цікавить, використовуючи спеціальне голосове меню, керуючи ним за допомогою натиснення клавіш в тоновому режимі або за допомогою голосу (при використанні технологій розпізнавання голоси) є IVR-системи. Вартість такої системи для підприємств складає біля 9800 грн. Передбачається його використання у кількості 1 одиниці.

3.1.1. Визначення витрат на підвищення інформаційної безпеки інтерактивної голосової служби

3.1.1.1 Визначення трудомісткості підвищення інформаційної безпеки інтерактивної голосової служби

Трудомісткість розробки визначається тривалістю кожної робочої операції:

$$t = t_{тз} + t_{в} + t_{а} + t_{з} + t_{м} + t_{р} + t_{д}, \quad \text{годин},$$

де $t_{тз}$ – тривалість складання технічного завдання, $t_{тз}=4$;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $t_{в}=14$;

$t_{а}$ – тривалість аналізу структури IVR–системи, $t_{а}=16$;

$t_{з}$ – тривалість визначення засобів реалізації обраного профілю захищеності, що враховує особливості інтерактивного голосового сервісу, $t_{з}=18$;

$t_{м}$ – тривалість будування матриці доступу співробітників до IVR–системи, $t_{м}=25$;

$t_р$ – тривалість розробки загальних рекомендацій організаційного характеру щодо захисту конфіденційної інформації в інтерактивних голосових системах, $t_р=11$;

$t_д$ – тривалість підготовки технічної документації, $t_д=5$.

Таким чином,

$$t = 4 + 14 + 16 + 18 + 25 + 11 = 88 \text{ годин.}$$

3.1.1.2. Розрахунок витрат на аналіз ефективності системи виявлення вторгнень інформаційно-телекомунікаційної системи

Витрати на створення програмного продукту Кпз складаються з витрат на заробітну плату виконавця програмного забезпечення *Ззп* і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 9856 + 69{,}8 = 9925{,}8 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 88*112 = 9856 \text{ грн.}$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_д \cdot С_{мч} = 5 \cdot 13{,}86 = 69{,}8 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 0{,}8 \cdot 10 \cdot 1{,}64 + \frac{2700 \cdot 0{,}5}{1920} + \frac{1300 \cdot 0{,}2}{1920} = 13{,}96 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = 5000 + 9800 + 9925{,}8 = 24725{,}8 \text{ грн.}$$

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{грн.}$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

Витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки ($С_в$) IVR–системи становлять близько 2800 грн. на рік.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів становлять 8000 грн.

Річний фонд амортизаційних відрахувань ($С_а$) визначається прямолінійним методом нарахування амортизації відповідно до строків їх корисного використання.

$$С_а = 9800 / 4 = 2450 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 14000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Отже,

$$С_з = 14000*12 + 14000*12*0,08= 181440 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2016 р. складає 22%.

$$С_{єв} = 181440 *0,22 = 39916,8 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=8,4 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$C_{ел} = 8,4*1920*1,64 = 26449,92 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 2% ($C_{тос} = 24725,8*0,02=494,52$ грн).

Витрати на керування системою інформаційної безпеки ($C_к$) визначаються:

$$C_к = 8000 + 2450 + 181440 + 39916,8 + 26449,92 + 494,52 = 258751,24 \text{ грн.}$$

Отже, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$C = 2800 + 258751,24 = 261551,24 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 10 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 7000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 9000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 5 осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 60 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 1,5 млн. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 5;

N – середнє число атак на рік, 30.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{7000 \cdot 60}{176} \cdot 4 = 9545{,}45 \quad \text{грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{7000 \cdot 60}{176} \cdot 10 = 23863{,}64 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_в = \frac{9000 \cdot 5}{176} \cdot 2 = 511{,}36 \text{ грн.}$$

$$П_в = 23863{,}64 + 511{,}36 = 24375 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються

виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{1500000}{2080} \cdot (4 + 2 + 10) = 11538{,}46 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 9545{,}45 + 24375 + 11538{,}46 = 45458{,}91 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_5 \sum_{30} 45458{,}91 = 6818836{,}72 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (25%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 6818836{,}72*0{,}25 - 261551{,}24 = 1443157{,}94 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{\text{E}}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{1443157{,}94}{24725{,}8} = 58{,}37, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (\text{N}_{\text{деп}} - \text{N}_{\text{інф}})/100),$$

де $\text{N}_{\text{деп}}$ – річна депозитна ставка, (18 %);

$\text{N}_{\text{інф}}$ – річний рівень інфляції, (12%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$58{,}37 > (18 - 12)/100 = 58{,}37 > 0{,}06.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{58{,}37} = 0{,}02 \text{, років.}$$

3.4 Висновок

Згідно із розрахунками економічної ефективності запропонованого підвищення інформаційної безпеки інтерактивної голосової служби можна вважати економічно доцільним. Коефіцієнт повернення інвестицій ROSI складає 58,37, що значно перевищує величину річної депозитної ставки з урахуванням інфляції, річний темп якої складає 12%. Термін окупності складає 0,02 років.

Економічний ефект від підвищення інформаційної безпеки інтерактивної голосової служби складе 1443157,94 грн.

ВИСНОВКИ

В результаті виконаного аналізу загроз в інформаційній системі IVR, був створений набір заходів захисту який включає в себе обрання необхідного профілю захищеності для даної системи та вибір засобів його забезпечення, запропонована матриця доступу для персоналу підприємства що взаємодіє з IVR та розроблені рекомендації що до захисту конфіденційної інформації яка циркулює в системі. Так як впровадження IVR-системи створює певний інноваційний ризик, то використання рішень запропонованих в дипломній роботі, допоможе зменшити його рівень, та створити надійну систему захисту інформації вже на початкових стадіях роботи. Розроблені заходи щодо захисту інформації можуть використовувати, як підприємства, що тільки впроваджують IVR-систему, так і підприємства, які вже давно використовують дане бізнес рішення, для підвищення рівня інформаційної безпеки.

Виходячи зі статистичних даних, можна сказати, що потреба в інтерактивних голосових системах з часом буде тільки зростати, бо більшість людей, запити яких були обслуговані за допомогою IVR, залишилися задоволеними. Також IVR-системи стають більш доступними, тобто їх створення і обслуговування може власноруч здійснювати компанія, яка потребує подібні рішення.

Автоматизація процесу обслуговування клієнта та зниження витрат завдяки цьому – є ще одним фактором, що сприяє розвитку інтерактивних голосових сервісів. Слід зазначити, що з розвитком технологій, IVR-системи будуть виконувати все більше різноманітних задач, разом з цим буде збільшуватися і обсяг інформації що в них циркулює. Тому необхідність забезпечення конфіденційності, цілісності, доступності та спостереженості інформації буде тільки зростати.

ПЕРЛІК ПОСИЛАНЬ

1 Гольдштейн Б.С., Фрейкнман В.А. Call-центры и компьютерная телефония. Научно техническое издание. - БХВ - Санкт – Петербург 2002. – 369 с.

2 Зачем нужны Call-центры(Електронний ресурс) / Спосіб доступу URL: http://vox-line.net/why-need-cc.php - Загол. з екрана.

3 Рынок call-центров 2009: готовность устоять против кризиса (Електронний ресурс) / Спосіб доступу URL: https://adm.cnews.ru/reviews/free/call2009/articles/construction.shtml - Загол. з екрана.

4 ISDN интерфейс PRI (Електронний ресурс) / Спосіб доступу URL: https://adm.cnews.ru/reviews/free/call2009/articles/construction.shtml - Загол. з екрана.

5 IP-телефония: основы и принципы. 1 часть - Технология будущого (Електронний ресурс) / Спосіб доступу URL: https://adm.cnews.ru/reviews/free/call2009/articles/construction.shtml - Загол. з екрана.

6 IP-телефония: основы и принципы. 1 часть - Технология будущого (Електронний ресурс) / Спосіб доступу URL: http://www.broadband.org.ua/content/view/377/489/1/1/ - Загол. з екрана.

7 IP-телефония. Обзор технологии (Електронний ресурс) / Спосіб доступуURL:http://newcom.com.ua/content/ru/articles/index.php?article=1- Загол. з екрана.

8 CRM (Електронний ресурс) / Спосіб доступу URL: http://www.kck.ru/kcksite/kcksite.nsf/search/B47AB81DFA6C95E2C3256C5B005425A3?Opendocument&ALT - Загол. з екрана.

9 Голос как инструмент управления. Требования к современной платформе IVR (Електронний ресурс) / Спосіб доступу URL: http://www.billing.ru/guest/node/303 - Загол. з екрана.

10 Плохой хороший IVR (Електронний ресурс) / Спосіб доступу URL: http://www.osp.ru/nets/2010/04/13001497/ - Загол. з екрана.

11 WideCoup Visual IVR (Електронний ресурс) / Спосіб доступу URL: http://rd.natec.com.ua/help/IVR/res/WideCoup_Visual_IVR_a.pdf - Загол. з екрана.

12 Вітлінський В.В., Верченко П.І. Аналіз, моделювання та управління економічним ризиком: Навч.-метод. посібник для самост. вивч. дисц. — К.: КНЕУ, 2000. — 292 с.

13 НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». - Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України - Київ 1999 – 53 с.

14 Комплекс «Гриф-Мережа»/ Описание (Електронний ресурс) / Спосіб доступу URL: http://www.ict.com.ua/?lng=1&sec=10&art=21- Загол. з екрана.

15 Tivoli Continuous Data Protection for Files (Електронний ресурс) / Спосіб доступу URL: http://www-142.ibm.com/software/products/ru/ru/ tivolicontinuousdataprotectionforfiles/- Загол. з екрана.

16 Межсетевые экраны Cisco ASA 5580 (Електронний ресурс) / Спосіб доступу URL: http://www.mototelecom.ru/katalog/setevoe-oborudovanie/mezhsetevye-ekrany/asa5580/- Загол. з екрана.

17 Установка и настройка Wine (Електронний ресурс) / Спосіб доступу URL:http://inc.istu.ru/index.php?option=com_content&view=article&id=1057:-wine&catid=90:instructioncat&Itemid=137- Загол. з екрана.

18 ДСТУ 3008-95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення.

19 24. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99р. № 22.

20 25. НД ТЗІ 2.5-005 -99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від "28" квітня 1999 р. № 22.

21 Кавун С.В. Інформаційна безпека : підручник / С.В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.

22 О.Г. Додонов, Д.В. Ланде, В.Г. Путятін. Інформаційні потоки в глобальних комп’ютерних мережах. – К.: Наук, думка, 2009. – 295 с.

23 Захист інформації в комп'ютерних системах та мережах: Методична розробка / Уклад.: Б.Я. Корнієнко, Л.М. Щербак . – К.: НАУ, 2006. – 64 с.

24 LinuxCenter (Електрон. ресурс) / Спосіб доступу: URL: http://www.linuxcenter.ru/. Загол. з екрана.

25 Вишняков В.М. Захист даних в інформаційних системах: навчальний посібник / В.М. Вишняков. – К.: КНУБА, 2010. – 128 с.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	30	
6	А4	2 Розділ	34	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Методи підвищення інформаційної безпеки інтерактивної голосової служби
студента групи 125м-17-1
Лісничого Владислава Олександровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, 25 джерел та 4 додатка.

Актуальність теми полягає в необхідності розробки комплексу засобів захисту для забезпечення безперервної роботи інтерактивної голосової служби CRM-системи контакт-центру.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатні рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі наведені особливості роботи та архітектура контакт-центрів, визначені переваги використання IP-телефонії, розглянуті основні функції інтерактивної голосової служби (IVR-системи), проведено аналіз загроз направлених на порушенні роботи інтерактивної голосової служби, розроблена модель порушника, обрано функціональний профіль захищеності, дані рекомендації щодо реалізації комплексу засобів захисту, побудована матриця розмежування доступу до IVR-системи, наведені рекомендації щодо використання платіжних карток VISA і MasterCard при замовлені послуг за допомогою IVR-системи.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Лісничий Владислав Олександрович заслуговує на оцінку «_____».

Керівник дипломної роботи,
к.ф.-м.н., проф. О.Ю. Гусєв

Керівник спец. част.,
ас. кафедри БІТ С.М. Мацюк