3 Технічні засоби системи захисту інформації. Стандартизація та метрологічне забезпечення систем ТЗІ. Визначення відповідності засобів ТЗІ

Юрій Хлапонін
Національний авіаційний університет
УДК 681.06

ОСОБЛИВОСТІ ВИНИКНЕННЯ КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ І НАВЕДЕННЯ

Анотація: ***Проведено аналіз утворення каналу витоку інформації за рахунок побічних електромагнітних випромінювань та наведень для різних компонентів персонального комп'ютера. Показано експериментально наявність небезпечного сигналу на частотах одиниць ГГц. Показана небезпека формування каналу витоку мовної інформації складовими комп'ютера,*** **що обробляє інформацію** ***та волоконно-оптичними лініями зв'язку.***
Summary: ***The analysis of the formation of information leakage through electromagnetic radiation and side are different components of a PC. It was shown experimentally availability dangerous signal at frequencies GHz units. Shown risk of formation of speech information leakage components of a computer that processes information and fiber optic lines.***
Ключові слова: ***Інформація, захист інформації, побічні електромагнітні випромінювання та наведення, інформативний сигнал.***

І Вступ

Одним з можливих каналів витоку інформації є випромінювання елементів комп'ютера, точніше, елементів основних технічних засобів (ОТЗ), якщо говорити про захищені автоматизовані системи (АС). Приймаючи і декодуючи ці випромінювання, можна отримати відомості про всю інформацію, що обробляється в комп'ютері. Цей канал витоку інформації називається ПЕМВН (побічного електромагнітного випромінювання і наведення). У Європі та Канаді застосовується термін „compromising emanation" – компрометуюче випромінювання. В Америці застосовується термін „TEMPEST" [1].

TEMPEST (скорочення від Transient Electromagnetic Pulse Emanation Standard) являє собою стандарт на перехідні електромагнітні імпульсні випромінювання працюючої радіоелектронної апаратури. Абревіатура TEMPEST з'явилася наприкінці 60-х початку 70-х років як назва секретної програми Міністерства Оборони США з розробки методів запобігання витоку інформації через різного роду демаскуючі і побічні випромінювання електронного обладнання.

Частотний діапазон побічних електромагнітних випромінювань, знаходиться в межах від одиниць кГц до 1 – 5 ГГц і визначається тактовою частотою використовуваного засобу обробки інформації. Слід відзначити, що ПЕМВН утворюються від небезпечного сигналу. **Небезпечний (інформативний) сигнал** містить, інформацію у відкритому виді [2].

Так, для стандартного комп'ютерного монітора перехоплення інформації можливе на частотах аж до 50 гармоніки тактової частоти, а рівень випромінювання, що становить в ближній зоні величину до десятків дБ, дозволяє приймати сигнали на відстані до декількох сотень метрів [3]. Крім електромагнітних випромінювань навколо засобів обробки інформації присутні квазістатичні інформаційні електричні і магнітні поля, що викликають наведення на близько розташовані кабелі, телефонні дроти, лінії охоронно-пожежної сигналізації, електромережу і т.п. Інтенсивність полів у діапазоні частот від одиниць кілогерц до десятків мегагерц така, що приймання сигналів може вестися за межами контрольованої зони (КЗ) при безпосередньому підключенні до цих ліній передачі.

Сучасні досягнення в області технології виробництва радіоприймальних пристроїв дозволяють створювати дуже мініатюрні чутливі приймачі. Успішно впроваджується багатоканальний прийом сигналів (як з різних напрямків, так і на різних частотах), з подальшою їх кореляційною обробкою. Це дозволило значно збільшити можливості перехоплення інформації. Особливо бурхливий розвиток ПЕМВН-технології отримали в кінці 80-х, початку 90-х років. Це пов'язано як з усвідомленням широкою

громадськістю небезпеки ПЕМВН загроз, так і з широким розвитком криптографії. Застосування при передачі інформації стійких алгоритмів шифрування часто не залишає шансів дешифрувати перехоплене повідомлення. У цих умовах ПЕМВН-атака може бути єдиним способом отримання хоча б частини інформації до того, як вона буде зашифрована.

При аналізі випромінювань шифрувальних машин було відмічено, що поряд з основним сигналом присутній і інший дуже слабкий сигнал. Шифрувальна машина, як і будь-яка інша електрична машина, має побічне електромагнітне випромінювання, яке модулюється інформаційним сигналом ще до моменту його кодування. Таким чином, при перехопленні і аналізі побічних випромінювань шифрувальної машини не маючи ключа для розшифровки кодованих повідомлень виникає можливість отримання інформації, що обробляється в інформаційній системі.

II Технологія Soft Tempest

Процес перехоплення конфіденційної інформації шляхом прийому паразитного випромінювання композитного сигналу монітора цілком реальний, але процес цей досить тривалий - потрібно дочекатися, поки користувач виведе на екран монітору цікаву конфіденційну інформацію. Такий процес може займати дні і тижні. Постає завдання змусити комп'ютер передавати потрібну інформацію і не чекати, поки користувач сам звернеться до конфіденційних документів, яка може бути вирішена наступним чином: потрібний комп'ютер „заражається" спеціальною програмою-закладкою («троянський кінь») будь-яким з відомих способів (за технологією вірусів: через компакт-диск з презентацією, цікавою програмою або іграшкою, дискету з драйверами, а якщо ПК в локальній мережі - то і через мережу). Програма шукає необхідну інформацію на диску і шляхом звернення до різних пристроїв комп'ютера викликає появу побічних випромінювань.

Така технологія отримала назву Soft Tempest – технологія прихованої передачі даних по каналу побічних електромагнітних випромінювань за допомогою програмних засобів, яка за своєю суттю є різновидом комп'ютерної стеганографії, тобто методу прихованої передачі корисного повідомлення в нешкідливих відео, аудіо, графічних і текстових файлах.

Методи комп'ютерної стеганографії в даний час добре розроблені і широко застосовуються на практиці. Особливістю технології Soft Tempest є використання для передачі даних каналу ПЕМВН, що значно ускладнює виявлення самого факту несанкціонованої передачі порівняно з традиційною комп'ютерною стеганографією. Дійсно, якщо для запобігання несанкціонованої передачі даних по локальній мережі або мережі Інтернет існують апаратні і програмні засоби (FireWall, Proxy server і т.п.), то **засобів для виявлення прихованої передачі даних по ПЕМВН немає, а виявити таке випромінювання в загальному широкополосному спектрі (більше 1000 МГц) паразитних випромінювань ПК без знання параметрів корисного сигналу вельми проблематично.**

Основна небезпека технології передачі конфіденційної інформації з використанням ПЕМВН полягає в скритності роботи програми-вірусу. Така програма на відміну від більшості вірусів не псує дані, що не порушує роботу ПК, не виробляє несанкціоновану розсилку по мережі, а значить, довгий час не виявляється користувачем та адміністратором мережі.

III Оптикоелектронна розвідка на службі TEMPEST

Одночасно з питанням прихованої передачі даних по каналу побічних електромагнітних випромінювань за допомогою програмних засобів (Soft Tempest) засобами розвідки може бути перехоплений світловий потік екрану монітора. Монітор має бути встановлений таким чином, щоб його не можна було розглянути через вікно або ж для огляду випадковими відвідувачами. Однак світловий потік екрану монітора відбивається від стін, і цей відбитий світловий потік може бути перехоплений. Сучасна техніка дозволяє відновити зображення на моніторі, прийняте після багаторазових відбиттів його від стін і всіх предметів [5].

IV Дослідження ПЕМВН складових ПЕОМ

Характер ПЕМВН визначається призначенням, схемними рішеннями, елементної базою, потужністю пристрою, а також матеріалами, з яких виготовлений корпус, і його конструкцією. **Випромінювання може відбуватися в широкому діапазоні частот (від одиниць Гц до ГГц)**, а дальність реального перехоплення інформації досягати сотень метрів.

Слід особливо відзначити, що застосування на ПЕОМ, яка призначена для обробки закритої інформації (тобто на ОТЗ) пристроїв, що використовують будь-які бездротові інтерфейси підключення (радіоканал, ІЧ-канал), крім волоконно-оптичних (ВОЛЗ), категорично заборонено. У зв'язку з цим „радіоклавіатури",

миші, ТВ-тюнери та іншу сучасну зручну периферію ми не розглядаємо принципово. Протоколи IR Wave, 802.11 (с будь-якими індексами), BlueTooth, Wi-Fi, WiMAX і т.д. заборонені в принципі.

Випромінювання монітора - дуже небезпечний канал витоку інформації. Так, DVI інтерфейс використовується в даний час як в LCD моніторах, так і в багатьох типах телевізорів. Назва роз'єму DVI походить від англійського скорочення Digital Visual Interface (цифровий відеоінтерфейс). Інтерфейс DVI був розроблений і впроваджений в 1999 році організацією Digital Display Working Group (DDWG) і заснований на форматі послідовної передачі даних (PanelLink). Кабель DVI складається з чотирьох кручених пар червоного, зеленого і синього кольорів, а також і clock (сигнал тактової частоти).

Перехоплення сигналів DVI цілком реальне. Хоча смугу пропускання приймача бажано б мати 200 Мгц в ідеалі. Тоді на частоті 1,2-2,5 Ггц, тобто проаналізувавши 9-10 гармоніки основної тактової частоти інтерфейсу DVI (точніше - HDMI 1.3) можна реалізувати перехоплення.

Існує загальна методика дослідження періодичних негармонічних сигналів (вхідних впливів і їх реакцій) в електричному ланцюзі, яка заснована на розкладанні сигналу в ряд Фур'є. Дана методика полягає в тому, що завжди можна підібрати ряд гармонічних (тобто синусоїдальних) сигналів з такими амплітудами, частотами і початковими фазами, алгебраїчна сума ординат яких в будь-який момент часу дорівнює ординаті досліджуваного несинусоидального сигналу. За відгуками практиків, ПЕМВН можна виявити, проаналізувавши 4-5 гармоніку сигналу на частоті приблизно 4 ГГц. Згідно з існуючими методиками пошук випромінювання, модульованого тестовим сигналом, здійснюється в діапазоні частот від 0,01 до 1000 МГц. В той же час тактова частота компонентів комп’ютера може становити одиниці Ггц. Для прикладу, жорсткі накопичувачі з інтерфейсом HDD SATA - 1500MHz, HDD SATA2 - 3000 MHz, HDD SATA-600- 4800 MHz.

Дослідження рівнів випромінювання, створюваних комп'ютерами в різних корпусах, що серійно випускаються, показали, що сучасні корпуси дозволяють значно послабити випромінювання елементів комп'ютера. Проте якість екранування корпусу системного блоку комп'ютера впливає на рівень випромінювання всіх пристроїв, підключених до системного блоку. Наприклад, клавіатура і монітор мають достатньо високий рівень випромінювання; вважається, що високий рівень випромінювань визначається наявністю у них сполучних кабелів. Це дійсно так, проте в серійних корпусів комп'ютерів не нормується ослаблення електромагнітного поля. Тому одна й та ж клавіатура або комплект „відеокарта - монітор - кабель” в різних корпусах можуть мати непередбачувано різний рівень випромінювань. Зокрема, на рис. 1.1 і рис. 1.2 наведено рівні електричної складової інформативних сигналів клавіатури і монітора відповідно. Дані, позначені як E1, E2 і E3, відносяться до трьох різних серійних корпусів [4].

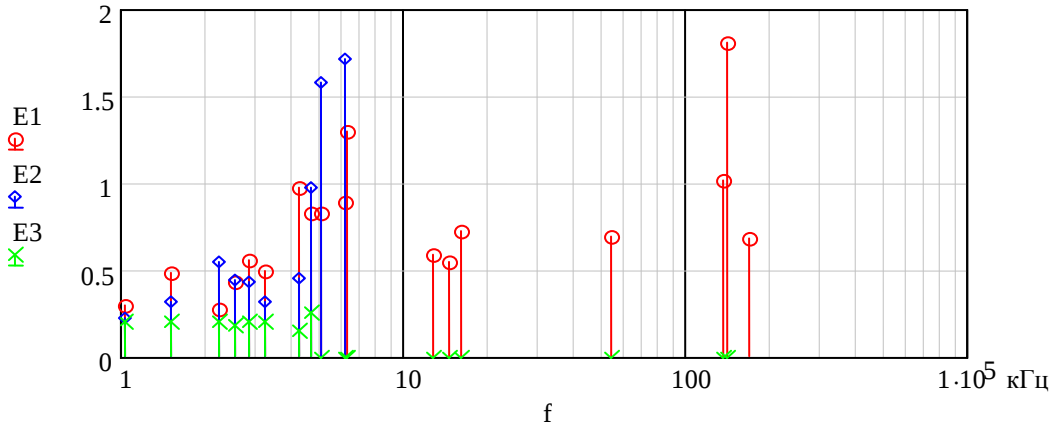

Рис.1.1 – Рівні електричної складової в режимі тестування клавіатури

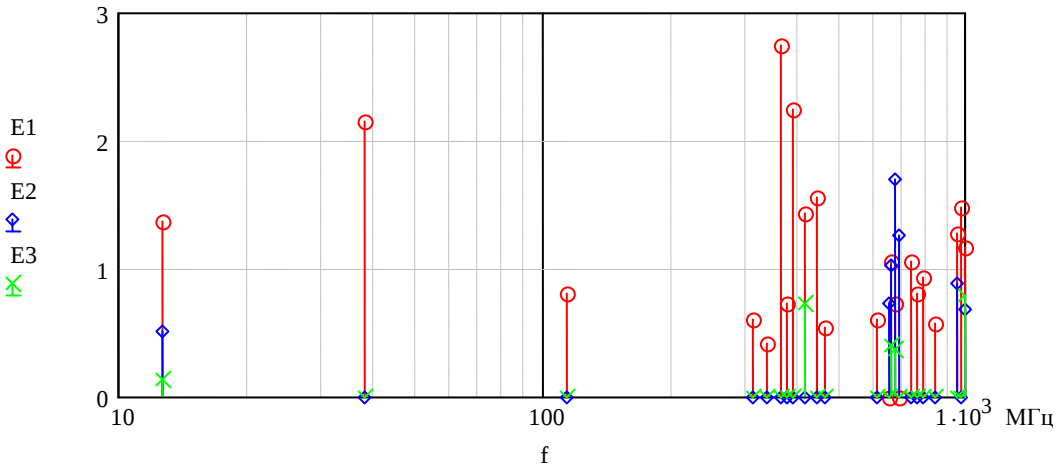

Рис.1.2 – Рівні електричної складової в режимі тестування монітору

З рис.1.2 можна зробити висновок, інформативність сигналів ПЕМВН суттєва на межі 1 Ггц, і постає питання необхідності спеціальних досліджень на частотах кількох Ггц, хоча методика цього не вимагає.

Аналогічні співвідношення виходять для всіх пристроїв, що входять до складу ПК.

V Наявність та якість заземлення технічних засобів

Для автономних пристроїв ЕОТ всупереч поширеній думці заземлення не відіграє визначної ролі щодо захисту інформації від витоку каналом ПЕМВН. Заземлення необхідно тільки за вимогами техніки електробезпеки.

Втім, через неідеальне екранування певний вплив заземлення все ж таки робить. Як правило, рівень побічних випромінювань при грамотно виконаному заземленні дещо знижується. Проте в деяких випадках при підключенні заземлення рівень побічних випромінювань може і збільшитися. Тому не можна однозначно стверджувати, що заземлення необхідно з точки зору захисту інформації від витоку по каналу ПЕМВН. Більше того, чим якісніше виконано екранування корпусу (включаючи і якість фільтрів в колах електроживлення), тим менше позначається на рівні побічних випромінювань наявність або відсутність заземлення.

Розділовий трансформатор пропонують [7] застосовувати також для захисту об'єктів ЕОТ від перешкод в двухпроводной мережі електроживлення за відсутності третього захисного проводу. Включення трансформатора і заземлення корпусу комп'ютера, усуває передачу небезпечних стрибків напруги перешкод з нульового проводу електромережі на металевий корпус комп'ютера. Природно, цей захист є ефективним на порівняно низьких частотах. Окремий провід заземлення - це і окремий канал поширення і перевипромінювання високочастотних сигналів, породжених електромагнітним полем даного комп'ютера. Цей сигнал поширюється в лінії, утвореній проводами електроживлення (включаючі і металевий корпус фільтра) і зворотним проводом, утвореним землею або металоконструкціями будівлі. Розміри еквівалентної лінії або антени - десятки метрів, її висота - одиниці метрів, тому ефективне перевипромінювання буде спостерігатися вже з частот порядку 1 МГц. Закриття проводів заземлення металевою трубою тільки збільшує ефективну довжину антени (антена Айзенберга [8]) і на високих частотах не забезпечує хорошого екранування.

VI Побічні випромінювання кабельної системи (мережі)

Кабельна мережа не містить активних і нелінійних елементів, тому сама по собі вона не може бути джерелом побічних випромінювань. Однак кабельна мережа пов'язує між собою всі елементи комп'ютерної мережі. Нею передаються мережеві дані, але разом з цим вона є також приймачем всіх наведень і середовищем для перенесення побічних електромагнітних випромінювань.

Слід розрізняти:

• побічне випромінювання, викликане сигналами, що передаються даною лінією (трафіком локальної мережі);

• прийом і подальше перевипромінювання побічних випромінювань від розташованих поблизу інших ліній і пристроїв;

• випромінювання кабельною системою побічних коливань від елементів мережевого активного обладнання і комп'ютерів, до яких підключений кабель.

Досить часто при оцінці захищеності кабельної системи цікавляться тільки тим, наскільки послаблюється побічне випромінювання, викликане сигналами, що передаються по кабелю в процесі мережевого обміну інформацією. Але в більшості практичних випадків кабельна система - це відмінна антена для всіх побічних випромінювань обладнання, підключеного до мережі. Побічні випромінювання, що виникають в елементах комп'ютера, наводяться на всі проводи кабелю локальної мережі. Поставити для цих проводів фільтр, що пригнічує побічні випромінювання, неможливо. Адже побічні випромінювання елементів комп'ютера (жорсткий диск, клавіатура тощо) зосереджені в тій же смузі частот, що і спектр імпульсів, переданих по кручений парі в процесі мережевого обміну. Пригнічуючи побічні випромінювання, ми придушимо і мережевий трафік. Таким чином, якщо комп'ютер із захистом інформації включити в локальну мережу на неекранованій витій парі, то проводи неекранованої витої пари, граючи роль антени, можуть підсилити напруженість поля, створюваного, наприклад, клавіатурою комп'ютера в десятки тисяч разів [7]. Тому неекранована вита пара не може застосовуватися в локальній мережі, в якій обробляється інформація з обмеженим доступом.

VII Комп'ютер як складова утворення каналу витоку мовної інформації

Комп'ютер може випромінювати в ефір і не тільки ту інформацію, яку він обробляє. Якщо при складанні комп'ютера не прийнято спеціальних заходів, то **він може служити також і джерелом витоку мовної інформації.** Це так званий „мікрофонний ефект". Ним може володіти навіть корпус комп'ютера. Під впливом акустичних коливань корпус трохи змінює свій об'єм, змінюються розміри щілин і інших елементів, через які здійснюється випромінювання. Відповідно випромінювання виходить модульованим і все, що ви говорите біля комп'ютера, може бути прослухано за допомогою приймача. Якщо ж до комп'ютера підключені колонки, то шпигун взагалі може добре заощадити на установці в ваших приміщеннях „жучків".

VIII Формування каналу витоку мовної інформації волоконно-оптичними лініями зв'язку

З точки зору захищеності інформації, ВОЛЗ вважаються ідеальними, оскільки в них відсутні випромінювання в радіотехнічному діапазоні частот. Але іншою є справа, коли розглянути прокладання ВОЛЗ поблизу або всередині виділених приміщень (об'єктів інформаційної діяльності), де проводяться конфіденційні (закриті) наради, засідання, обговорення. Тоді з'являється загроза витоку мовної інформації з обмеженим доступом (ІзОД) через саму структуру волоконно-оптичного кабеля (ВОК) [9].

У випадку ВОЛЗ, на відміну від відомих прикладів акустоелектричних перетворень, може здійснюватись модуляція електромагнітної хвилі оптичного діапазону. Ця модуляція не впливає на передачу цифрових сигналів, але дозволяє перехопити мовну інформацію, яка циркулює в приміщенні, через яке проходить ВОЛЗ. Таким чином, у ВОЛЗ, в силу їх конструктивних особливостей, виникає можливість каналу витоку мовної інформації за рахунок акустоелектричних перетворень.

IX Висновки

В статті розглянуті особливості виникнення каналу витоку інформації за рахунок побічного електромагнітного випромінювання і наведення та показано як засіб ЕОТ, що обробляє інформацію (ОТЗ) може стати джерелом витоку мовної інформації за рахунок так званого „мікрофонного ефекту". Показано, що кабельна система може бути відмінною антеною для всіх побічних випромінювань обладнання, підключеного до мережі, а ВОЛЗ може слугувати лінією витоку мовної інформації за рахунок акустоелектричних перетворень.

Список використаної літератури: ***1.*** *Markus G. Kuhn, Ross J. Anderson. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations / University of Cambridge, Computer Laboratory, New Museums Site, Pembroke Street, Cambridge CB2 3QG, United Kingdom, fmgk25,rja14g@cl.cam.ac.uk.* ***2.*** *Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: Арий, 2010. – Том I. Несанкционированное получение информации. – 464 с.* ***3.*** *Пятачков А.Г. Защита информации, обрабатываемой вычислительной техникой, от утечки по техническим каналам /А.Г. Пятачков. М.: НП РЦИБ «Факел», 2007.* ***4.*** *http://www.epos.ua/view.php/ aboutpubs _archive? Subaction =showfull&id=1037743200&archive=&start_from=&ucat=2&.* ***5.*** *Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays/ University of Cambridge, Computer Laboratory, JJ Thomson Avenue, Cambridge CB3 0FD, UK, mgk25@cl.cam.ac.uk* ***6.*** *Анализ защиты компьютера от утечки по цепям питания и заземления. Стеченко В. Н., Найденко В. І., Прокофьев М. И., Курашкевич А. /Правове, нормативне та метрологічне забезпечення системи захисту інформації в україні, вип. 1(14), 2007 р. 165.* ***7.*** *ГОСТ Р 50571.22-2000 Электроустановки зданий. Требования к специальным электроустановкам. Заземление оборудования*

обработки информации. ***8.*** *Айзенберг Г. З. и др. Коротковолновые антенны. М.: Радио и связь, 1985.* ***9.*** *Гришачев В. В., Халяпин Д. Б., Шевченко Н. А. Опасности возникновения каналов утечки конфиденциальной речевой информации по волоконно-оптическим структурированным кабельным системам // Материалы X Международной научно-практической конференции „Информационная безопасность”. Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2008. –103 – 105 с.*

Владимир Темников, Игорь Конфорович, Елена Темникова*
*Национальный авиационный университет, *Национальный технический университет Украины «Киевский политехнический институт»*

УДК 004.93

ПОСТРОЕНИЕ ГОЛОСОВОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ ДИСПЕТЧЕРОВ С ПОВЫШЕННЫМИ БЫСТРОДЕЙСТВИЕМ И ДОСТОВЕРНОСТЬЮ РАБОТЫ

Аннотация: **Представлены концепция построения и структура разработанной авторами автоматической голосовой системы перманентной аутентификации диспетчеров во время выполнения ими своих профессиональных обязанностей. Задачей системы является предотвращение доступа несанкционированных лиц к информационным ресурсам, используемым диспетчерами в процессе работы. Приведены использованные при построении системы способы повышения быстродействия и достоверности ее работы. Применение искусственных нейронных сетей и разработанной системы информативных параметров речевых сигналов, обоснованный выбор значений параметров позволили обеспечить функционирование системы аутентификации в режиме реального времени при высокой степени достоверности ее работы (процент правильной аутентификации выше 98%).**

Summary: **The article presents the concept of construction and structure of the authors' automated voice system of permanent traffic-controllers authentication during the performance of their professional duties. The objective of the system is preventing of unauthorized persons access to information resources used by controllers in the process. The article describes ways to improve the speed and reliability of the system.**

The application of artificial neural networks and developed system of informative parameters of speech signals, grounded choice of parameter values enabled the operation of the authentication system in real time with a high degree of reliability of its work (the percentage of correct authentication above 98%).

Ключевые слова: **Система аутентификации, диспетчеры, искусственные нейронные сети, параметризация речевых сигналов.**

I Введение

Одной из основных причин аварий и аварийных ситуаций на транспорте и в энергетике является человеческий фактор. Так, опубликованные в литературе статистические данные свидетельствуют о том, что, например, до 80% всех аварий и нарушений технологического режима в авиации происходят по вине диспетчерского персонала. Ошибки в его работе в значительной степени обусловлены нахождением диспетчеров в состоянии перманентного напряжения, связанного с ответственностью за жизнь людей и возможные значительные материальные потери.

Учитывая, что в настоящее время за диспетчерами осуществляется лишь визуальный контроль со стороны старшего диспетчера (администратора), авторы предлагают снижать влияние человеческого фактора на безопасность путем введения голосового автоматического контроля за действиями диспетчеров и их психофизиологическим (эмоциональным) состоянием. Предполагается, что система контроля доступа (СКД) диспетчеров к информационным ресурсам, используемым диспетчерами в процессе работы, будет функционировать в режиме реального времени и своевременно сигнализировать о нарушениях в работе диспетчеров, а отчет о ее работе будет служить документальным подтверждением факта нарушения.

В известной авторам литературе отсутствует информация о системах, которые бы в автоматическом режиме осуществляли высокоточную аутентификацию, идентификацию и контроль психофизиологического (эмоционального) состояния человека и, при этом, работали в режиме реального времени.

Использование голоса в качестве анализируемого образа дает возможность осуществлять контроль диспетчеров бесконтактно, дистанционно, не отвлекая их от работы.

В настоящей статье представлена концепция построения автоматической голосовой системы аутентификации диспетчеров (САД), являющейся частью разрабатываемой комплексной автоматической СКД диспетчеров к информационным ресурсам, обеспечивающей проведение перманентных