На рис. 5 показана структура обобщенной ГИС в виде трехуровневой системы. По этим уровням можно проводить сравнение различных ГИС.

Выводы

В статье рассмотрены геоинформационные технологии и место ГИС-компонент при решении телекоммуникационных задач. Предложена структура обобщенной ГИС в виде трехуровневой системы, по которым можно проводить сравнение различных ГИС.

Список литературы: **1.** *Берлянт, А. М.* Телекоммуникационное картографирование [Текст]/ *А. М. Берлянт* // Вестн. Моск. ун-та. Сер.5. География. –1997.– №3. **2.** *Берлянт, А. М.* Картография и телекоммуникация (аналитический обзор) [Текст]/ *А. М. Берлянт* // – М.: Астрея, 1998. **3.** *Митчелл Э.* Руководство по ГИС-анализу [Текст]. – Киев: ЗАО УСОММСо, 2000. – Ч.1.

Надійшла до редколегії 20.12.2012

УДК 044.03

Использование геоинформационных технологий в телекоммуникации/ Штангей С. В. // Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. – Х: НТУ «ХПІ», – 2012. - № 68 (974). – С. 122-127. – Бібліогр.: 3 назв.

Проведено аналіз ГІС, як складної системи. розглянуті геоінформаційні технології та місце ГІС-компонент при вирішенні телекомунікаційних завдань. Запропоновано структуру узагальненої ГІС у вигляді трирівневої системи, за якими можна проводити порівняння різних ГІС. .

Ключові слова: Геоінформаційні системи, бази даних, телекомунікації, геоінформація, платформа ArcGIS.

The analysis of the GIS as a complex system. considered GIS technology and place GIS component in solving telecommunication problems. The structure of the GIS in the form of a generalized three-level system, which you can make a comparison of different GIS.

Keywords: GIS systems, databases, telecommunications, geoinformation, ArcGIS platform

УДК 004.77

П. О. СИДОР, директор ПП «Пожспецтех-захід», Чернівці

ПРОБЛЕМИ ТА ШЛЯХИ ПОДОЛАННЯ ПЕРЕШКОД ПЕРЕДАЧІ СПОВІЩЕНЬ ЗАСОБАМИ ОХОРОННО-ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ

Проведено аналіз сучасного стану захисту охоронних комплексів. Встановлено шляхи оптимізації витрат охоронних підприємств.

Ключові слова: охоронна система, сигналізація, пульт централізованого спостереження, безпека об’єкту, радіозавада.

Постановка проблеми

В умовах сьогодення особливої актуальності і гостроти набуває питання технічної охорони різноманітних об’єктів, оскільки технічні засоби, як і засоби протидії охоронним системам, модернізуються швидкими темпами. Від рішення цього питання багато в чому залежить цілісність майнових комплексів, ефективність використання засобів охорони, що обумовлено сучасним рівнем розвитку науки і техніки. Проте засоби (канали) зв’язку для передачі тривожних та інших сповіщень від приладів охорони до пультів центрального спостереження не вдосконалюються. Тому постає проблема достовірності і своєчасності надходження інформації, її захищеності від засобів ефективної протидії засобам блокування зловмисників.

Метою роботи є аналіз сучасного стану захисту охоронних комплексів.

Виклад основного матеріалу

Більшість засобів технічної охорони використовують сучасні канали передачі інформації через комутовані канали CSD і з пакетною передачею GPRS (EDGE, EVDO). Також широко використовуються канали передачі технології CSD через GSM, що

насправді є удосконаленим засобом використання технології передачі незайнятими комутованими лініями телефонії загального призначення. В свою чергу, це вирішило проблему пошкодження телефоних ліній (кабелів) та втрати каналів зв'язку пультом центрального спостереження з абонентськими приладами. Час надходження та передачі інформації може збільшуватись до 2-5 хвилин, що обумовлює особливості даної технології (дозвону на номера ПЦС і періоди повторного набору номера).

При сучасному розвитку технологій почали широко використовуватись канали з пакетною передачею GPRS (EDGE, EVDO) [1]. Також для відмовозахисту почали застосовуватись дублюючі або резервні модуля CSD / GPRS (EDGE, EVDO) через GSM або CDMA стандарти зв'язку, з використанням різних операторів мобільного зв'язку. Або механізми переключення з більш швидкого GPRS до більш надійного але повільнішого CSD. Використання технологій CSD або GPRS не дозволяє бути впевненим, що зловмисники не отримають дублікат карти з відповідним номером або не згенерують хибний IP пакет. Втрачається достовірність інформації, вона може легко бути спотворена або підмінена на таку, яку хоче зловмисник [2,3]. Засоби контролю та криптостійкі системи на сьогодні не використовується та в вільний продаж не надходять. Єдиний засіб криптостійкості, це закритись інформації відносно протоколу, наприклад ГЛОБУС і т.д. . А ті протоколи в яких почали використовувати криптографічні методи не використовує сучасні криптографічні алгоритми, ставшими стандартами захисту інформації в світі. Так використання алгоритмів AES, DES, 3DES вона повина забезпечуватись окремим модулем або контролером. PIC контролери, які використовуюь в сучасних охороних приладах не мають достатньої обчислювальної потужності. А час на виконання цих операцій буде відносно великий, що не дозволить функціонувати основній системи ОПС. Багатозадачних систем як в сучасних засобах техніки нажаль не використовуютьв приладах ОПС так, як це підвищить їх вартість в рази. Можно констатувати, що інформаційні повідомлення передаються в деяких системах не в закритому вигляді, але не є достатньо захищеними.

Також необхідно звернути увагу на те, що зловмисник може здійснити атаку типу «відмова в обслуговуванні» звичайним пристроєм шуму в діапазоні 800-2100 Mhz, сьогодні вартість зазначених пристроїв (рис.) становить менше 400 грн., їх можливо придбати в більшості спеціалізованих інтернет-магазинів. Дана методика атаки досить ефективна, оскільки вона блокує роботу радіозавадами на невеликому визначеному просторі з більшою потужністю радіозавади, ніж корисний радіосигнал передачі інформації, що унеможливлює роботу приймачів або передавачів охоронних приладів. Даний тип атаки не враховується зовсім охоронними підприємствами, але є найменш затратним та найбільш ефективним, ніж спотворення чи підміна. Цей тип атаки є найбільш імовірним засобом блокування сповіщень охоронно-пожежної сигналізації, оскільки не залишає слідів втручання завдяки використанню принципу зашумлення радіочастотного ефіру.

Рис. – Пристій генерації шуму 800-2100Mhz

При детальному аналізі радіочастотного спектру можна помітити постійну шумоподібну заваду досить високої потужності з чіткими фронтами, що унеможливлює роботу охоронних приладів, мобільних телефонів та інших приладів стандартів GSM, CDMA, iDEN незалежно від оператора зв'язку. Тому впровадження 2 стандартних систем CSD / GPRS (EDGE, EVDO) або дублюючих (резервних) прийомо-передавачів CSD / GPRS (EDGE, EVDO) для надійності і своєчасності сповіщення (в охоронній галузі кожна секунда здатна зберегти життя або припинити протиправні посягання на об'єкт охорони) не вирішують проблеми. Навіть при спрацюванні технічного засобу він не зможе передати

повідомлення про спрацювання (порушення політики безпеки).

Використання даного принципу атаки дозволяє здійснити протиправні дії, наприклад, винести термінал самообслуговування (банкомат) безперешкодно. Корисне інформаційне повідомлення про протиправні дії ніколи так і не потрапить на пульт ПЦС, незалежно від використання двох стандартних модулів CSD / GPRS (EDGE, EVDO) або двох модульних систем з використанням послуг різних операторів зв'язку.

Як зазначає професор Б.В. Кузьменко, загроза кібератак стала реальною, а її ризики оцінюються як достатньо високі. Використання мережевого інструментарію здатне вивести з ладу критичні компоненти національної інфраструктури (енергетичні потужності держави, зв'язок, транспортні, фінансові та інші засоби). Реальне оцінювання відповідного ризику передбачає необхідність визначення успішного здійснення кібератаки та обсягів можливих збитків. У зв'язку з цим, доцільним є також урахування "людського фактора" та "інсайдерської інформації", методів аналізу та управління ризиками, захисту інформації, що дають змогу адекватно оцінювати такий перебіг подій, у тому числі вияви кібертероризму. Проте фахівців у цій сфері досить мало, як і тих, хто здатний застосувати ці методи на практиці. Отже, нагальним є питання постановки і вирішення завдань з аналізу й управління ризиками для адекватного оцінювання реальності виявів кібертероризму та підготовки фахівців у цій галузі. Актуальним також є завдання проведення наукових досліджень у відповідному напрямі. Сучасні світові та українські реалії свідчать про те, що кібератаки можуть мати серйозні наслідки, хоч і не завжди пов'язані із заподіянням збитків життю і здоров'ю людей [4].

Проаналізувавши статистику відмов ОПС та виявивши відсутність подачі сповіщень, які раніше визначали як несправність засобу ОПС попередніх років, технічні спеціалісти зможуть виявити, що зловмисники вже давно користуються даним типом атак. Служби охорони ігнорують ці атаки та не протидіють їм в силу своєї технічної необізнаності.

Суть даної технології полягає в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже встановленому з'єднанні організується шифрований канал, що забезпечує високий рівень захисту переданої з цього каналу інформації за рахунок застосування спеціальних алгоритмів шифрування. Використання технології VPN необхідно там, де потрібен захист корпоративної мережі від дії вірусів, зловмисників, некомпетентних користувачів, а також від інших загроз, які є результатом помилок в конфігурації або адміністрування мережі [5].

Можна зробити висновок, що ігнорування проблеми та замовчування шляхів подолання, аналізу відмов засобів ОПС в охоронній діяльності завжди закінчуються з визначеним заздалегідь результатом і, як правило, не на користь охоронних підприємств. Особливої гостроти піднятій проблемі надає той факт, що даний недолік притаманний 99,9% відсотками охоронних систем в Україні. Про кількість дійсних причин заволодіння майном та обходу (блокування) систем ОПС можна лише здогадуватись.

Отже використання пакетної передачі інформації збільшує швидкість передачі інформації. Для збільшення швидкості та використання іншої технології каналоутворюючого обладнання можливо використовувати IP (Ethernet) модуля. З протоколом IP ми стикаємось майже кожний день, саме він і є тією технологією, яка дозволила створити INTERNET. А використання віртуальних приватних мереж (VPN) дозволить будувати захищені тунелі від приладів ОПС до пультів ПЦС, що унеможливить втручання, підміну або спотворення інформації. Також VPN-технологія дозволить використовувати існуючі публічні і приватні мережі, враховуючі те, що більшість інфраструктури мереж вже побудована, треба лише використати її, що зменшує вартість впровадження. Втрата VPN тунелю може бути відслідкована протягом декількох секунд [6]. Також завжди втрату тунелю можна розцінювати, як втручання в канал зв'язку або використання зловмисниками технічних засобів протидії. Економічний аспект

впровадження модулів Ethernet та VPN буде завжди менш затратним, ніж заміна абонентського приладу повністю, та більш ремонтно придатним завдяки модульності системи [7]. Можливо оптимізувати витрати охоронних підприємств шляхом запровадження основного каналу зв'язку по IP (TCP/UDP), а дублюючого або резервного за необхідністю CSD / GPRS (EDGE, EVDO).

Висновок

Показано, що з вищевикладеного тільки використання систем за різними технологіями, які дублюють одна одну (резервні), дасть змогу підвищити надійність та достовірність переданої інформації. Запропоновано використання IP (Ethernet) модулів для вирішення проблеми, що дасть змогу анулювати проблему атак типу «відмова в обслуговуванні».

Список літератури: **1.** Олифер В. Г. , Олифер Н. А . Компьютерные сети. Принципы, технологии, протоколы. Издание 4-ое. / *Олифер В. Г. , Олифер Н. А .*/ Питер, 2010. – 943 с. **2.** *Макаренко Є. А.* Міжнародна інформаційна безпека: сучасні виклики та загрози / *Макаренко Є. А., Рижиков М. М., Ожеван М. А.* – К. : Центр вільної преси, 2006. – 916 с. 3. *Таран А. В.* Классификация информационных угроз современному обществу / А. В. Таран [Электронный ресурс]. — Режим доступа : http://www.humanities.edu.ru/db/msg/88048. **4.** *Кузьменко Б. В.* Кібертероризм: світові й українські реалії / *Б. В. Кузьменко, Ю.О. Заїка* // Науковий вісник Національної академії внутрішніх справ. – 2012. – С. 92-98. **5**. *Пархоменко І. І.* Переваги застосування технологій VPN в корпоративних мережах / *І. І. Пархоменко, О. О. Квачук* // Авіа – 2011 : Матеріали X Міжнародної науково-технічної конференції. – Національний авіаційний університет, 19-21 квітня 2011. – К., 2011. – С. 12-13. **6**. Military and Security Deployments Involving the People's Republic of China // [Електронний ресурс]. — Режим доступу : http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf **7**. *Krasavin S.* What is Cyber-terrorism? / S. Krasavin [Електронний ресурс]. — Режим доступу : www: sans.org/infowar.

Надійшла до редколегії 20.12.2012

УДК 004.77

Проблемы и пути преодоления препятствий передачи сообщений средствами охранно-пожарной сигнализации/ Сидор П. О. // Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. – Х: НТУ «ХПІ», – 2012. - № 68 (974). – С. 127-130. – Бібліогр.: 7 назв.

Проведен анализ современного состояния защиты охранных комплексов. Установлено пути оптимизации расходов охранных предприятий.

Ключевые слова: охранная система, сигнализация, пульт централизованного наблюдения, безопасность объекта, радиопомеха.

Analysis of the current state of security protection systems is conducted. Ways of optimization the cost of security companies are found.

Keywords: burglar alarm system, alarm, central monitoring system, security object, interference.

УДК 004.931 : 621.372.542

О. О. ФРАЗЕ-ФРАЗЕНКО, заст. нач., Центр інформаційних технологій, ОНЕУ, Одеса

КОМПЕНСАЦІЯ КРАЙОВИХ ШУМОВИХ СПОТВОРЕНЬ НА ЦИФРОВОМУ ЗОБРАЖЕННІ

У статті розглядається метод компенсації шуму та шумових спотворень на цифровому зображенні. Метод передбачає використання спрощеної процедури та може бути використаний для підвищення якості виділення контурів в системах захисту інформації, де при ідентифікації та аутентифікації використовується термограма лиця особи.

Ключові слова: ідентифікація, аутентифікація, контур, зображення, шум, термограма, дифузія.

Вступ

У системах захисту інформації, які забезпечують доступ до інформаційних ресурсів, ідентифікація по обличчю людини є біометричною технологією, яка не є найбільш