Короткі повідомлення

УДК 638.235.231

АНАЛІЗ МІЖНАРОДНОГО СТАНДАРТУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ISO 17799 ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ ЙОГО В УКРАЇНІ

Павло Курбет
Спеціальний факультет СБ України ВІТІ НТУУ "КПІ"

Анотація: **Наведено аналіз міжнародного стандарту з інформаційної безпеки ISO 17799.**
Summary: **Analysis of international standard from informative safety of ISO 17799.**
Ключові слова: **Інформаційна безпека, міжнародний стандарт.**

На сьогоднішній день існує певна невизначеність у оцінці захищеності інформаційних систем. Це питання є важливим у сфері інформаційної безпеки і тим самим "тонким" місцем, якого зазвичай прагнуть уникати фахівці. І дійсно, оцінити захищеність інформаційної системи досить складно, але, як відомо, можна. Для цього існують в основному якісні методи оцінки рівня захищеності, які на виході дозволяють отримати не кількісну оцінку ("система захищена на 4,2 балів або на 58%"), а якісну – система відповідає певному класу або рівню захищеності; тому або іншому стандарту безпеки, наприклад, за НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.", затверджено наказом ДСТСЗІ СБ України від 28. 04. 99 р. № 22, чинний від 01. 07. 1999 р. Кількісні методи оцінки на практиці не знайшли свого застосування. Застосування якісних методів оцінки є на сьогоднішній день єдиним способом отримати уявлення про реальний рівень захищеності інформаційних ресурсів організацій [1].

Перейдемо до наступної частини і зазначимо, яке питання зазвичай є ключовим при проведенні аудиту безпеки. Звичайно це питання про стандарт безпеки, перевірку на відповідність якому виконуватиме аудитор. У Росії, наприклад, звичайною практикою при проведенні аудиту є виконання даних робіт без прив'язки до якого-небудь критерію або стандарту – аудитор обмежується оцінкою поточного рівня захищеності і виробленням рекомендацій з його підвищення відповідно до своєї експертної оцінки і свого розуміння про рівні і критерії захисту. І, загалом, це нормальна практика, коли компанія довіряє вибраному експертові або групі експертів, але проводити аудит, грунтуючись тільки на власній експертній оцінці, не враховуючи світовий досвід і існуючі стандарти безпеки, на сьогоднішній день практично неприпустимо. Проаналізуємо такий стандарт безпеки як ISO 17799.

В 1993 році Британський інститут стандартів (BSI) за участю комерційних організацій, таких як Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica і інших, зайнявся розробкою стандарту інформаційної безпеки. І в 1995 р. був прийнятий національний стандарт BS 7799 з управління інформаційною безпекою організації незалежно від сфери її діяльності. Служба безпеки, IT-відділ, керівництво компанії починають працювати згідно з загальним регламентом. Неважливо, йдеться про захист паперового документообігу чи електронних даних. Британський стандарт BS 7799 підтримується в 27 країнах світу, в числі яких країни Британської Співдружності, а також, наприклад, Швеція і Нідерланди. У 2000 р. міжнародний інститут стандартів ISO на базі британського BS 7799 розробив і випустив міжнародний стандарт менеджменту безпеки ISO/IEC 17799. Тому сьогодні можна стверджувати, що BS 7799 і ISO 17799 – це один і той же стандарт, що має на сьогоднішній день світове визнання і статус міжнародного стандарту ISO. Остання модернізація стандарту ISO 17799 проведена в 2005 році [2].

Приведемо основні розділи стандарту ISO 17799:

Передмова
Вступ
Що таке інформаційна безпека?
Навіщо потрібна інформаційна безпека
Визначення вимог до безпеки
Оцінка ризиків, пов'язаних з інформаційною безпекою
Вибирання засобів захисту

Основа інформаційної безпеки
Ключові чинники успіху
Розробка власних правил
1 Область застосування
2 Терміни і визначення
3 Політики безпеки
4 Організаційна безпека
5 Класифікація і контроль ресурсів
6 Питання безпеки, пов'язані з персоналом
7 Фізична безпека і захист територій
8 Забезпечення безпеки при експлуатації
9 Контроль доступу
10 Розробка і обслуговування систем
11 Забезпечення безперервності бізнесу
12 Відповідність вимогам.

Останнім часом ISO 17799 почав упевнено просуватися країнами СНД. У Молдові завдяки позиції Національного банку всі банки проходять регулярну перевірку на відповідність ISO 17799. У Росії стандарт ISO 17799 поки не має статусу державного стандарту. Проте останнім часом ситуація змінюється: Державна технічна комісія при Президентові РФ вже відмовилася від використання власних стандартів захищеності автоматизованих систем і прийняла ГОСТ 15408 (ISO 15408). Очікується, що подібна ситуація найближчими часом в Росії відбудеться і з ISO 17799, і нам слід чекати появи ГОСТ 17799. В Україні також існують плани з впровадження даного стандарту, адже він є певним і чітко визначеним алгоритмом з побудови системи інформаційної безпеки будь-якої організації та має ряд суттєвих переваг, які будуть визначені нижче. Офіційним представником в Україні даного стандарту є фірма Digital Security, яка проводить низку навчальних програм та семінарів з вивчення ISO 17799. Які переваги отримує компанія, яка провела аудит безпеки своїх інформаційних ресурсів і отримала сертифікат відповідності системи управління інформаційної безпеки за стандартом ISO 17799?

Перш за все – це "неформальні" переваги: після проведення аудиту інформаційна система компанії стає "прозорішою" для менеджменту, виявляються основні погрози безпеці для бизнес-процесів, виробляються рекомендації з підвищення поточного рівня захищеності для захисту від виявлених загроз і недоліків в системі безпеки і управління. В результаті компанії пропонується комплексний план внесення змін в систему управління інформаційною безпекою як для підвищення реального рівня захищеності, так і для безпосередньої відповідності стандарту.

Сертифікація на відповідність стандарту ISO 17799 (BS 7799) дозволяє наочно показати діловим партнерам, інвесторам і клієнтам, що в компанії налагоджено ефективне управління інформаційною безпекою. В свою чергу, це забезпечує компанії конкурентну перевагу, демонструючи здатність управляти інформаційними ризиками.

Крім того, кажучи про сертифікацію по ISO 17799, варто прийняти до уваги узгоджену з ВТО процедуру ухвалення вступу в дану організацію. Ця процедура зажадає адекватної реакції від найбільш значущих в економіці структур і адаптації стратегії розвитку в області інформаційних технологій з урахуванням міжнародних стандартів безпеки, таких як ISO 17799.

Для отримання сертифікату відповідності ISO 17799 компанія повинна пройти аудит інформаційної безпеки, провести підготовку інформаційної системи на відповідність стандарту, впровадити зміни і провести остаточну перевірку відповідності стандарту. Дану роботу доцільно розбити на декілька етапів.

Попередній етап полягає в проведенні аудиту і на його підставі підготовці необхідних змін системи управління інформаційною безпекою. Його може виконати спеціалізована організація, що має досвід з проведення подібних робіт. Потім, після підготовки комплекту необхідних документів і внесення змін в систему, необхідно провести підсумкову перевірку відповідності ISO 17799, для чого потрібна участь фахівців однієї з консалтингових компаній, які володіють ексклюзивним правом видачі даного сертифікату і мають акредитацію при UKAS (United Kingdom Accreditation Service), – уповноваженому державному органі Великобританії.

Для вирішення завдання створення і перевірки політики інформаційної безпеки компанії застосовуються наступні програмні комплекси: британська Cobra (компанія C&A Systems Security Ltd.) і російський КОНДОР (компанія Digital Security). Британська "Кобра" від компанії C&A Systems Security Ltd. є продуктом, що дозволяє аудиторові провести перевірку відповідності інформаційної системи вимогам ISO 17799. "Кобра", як і будь-який продукт даного класу, є експертною системою, завдання якої, опитавши IT-менеджера, зробити висновок про відповідність системи ISO 17799.

З огляду на зазначене вище можна зробити висновок, що міжнародний стандарт ISO 17799 має бути одним з керівних документів у сфері інформаційної безпеки в Україні та перевірки відповідності систем захисту інформаційних ресурсів вимогам зазначеного стандарту, що дасть змогу привести їх до світових стандартів. Важливим чинником у підвищенні рівня інформаційної безпеки організацій є створення національних програмних комплексів для перевірки відповідності не лише міжнародному стандарту, але і всій ситемі керівних документів України з питань інформаційної безпеки.

Література: ***1.*** *НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".* ***2.*** *International standard ISO/IEC 17799.*

УДК: 621.396.677.4;[539.37.38:621.396.946]

РАДІОПЕЛЕНГАЦІЙНА АНТЕНА UNF ДІАПАЗОНУ

Ігор Курбатов, Юрій Міць
Запорізький національний університет

Анотація: **Розглядається новий практичний напрямок формування зовнішних полів випромінювання (діаграм спрямованості) в окремій спіральній структурі.**
Summary: **New practical direction of forming of external fields of emanation in the separate spiral structure was considered**
Ключові слова: **Спіральна антена, поверхові хвилі, діаграма спрямованості, смуга частот, радіопеленгація, радіонавігація, радіорозвідка, радіоборотьба.**

I Вступ

Налагодження методичної боротьби з витоком конфіденційної інформації з електронних інформаційних систем сприяє ефективній боротьбі з хабарництвом, корупцією, організованою злочинністю, а особливо з тероризмом і є сучасним найважливішим та найактуальнішім напрямком розвитку політичної та економічної незалежності України. Ефективність такого напрямку залежить від використання спеціальних сучасних та мобільних радіотехнічних систем оперативного *вимірювання точних координат* користувачів електронних приладів незалежно від місця розташування джерел випромінювання.

Ефективність приймання випромінювання в умовах зовнішніх завад залежить від здатності пристроїв формувати в дальній зоні поля в найширшій смузі робочих частот із заданими радіопеленгаційними характеристиками.

II Постановка задачи

Розробка спеціальної апаратури виявлення відповідних ефірних сигналів, точного електронного радіостеження за ними та безперервного виміру їхніх координат *стримується*, головним чином, не відсутністю відповідних радіотехнічних засобів прослуховування або радіопеленгування, а *відсутністю малогабаритних широкосмугових* ***спеціальних антен*** *зі спрощеними системами регулювання зовнішніх радіопеленгаційних характеристик та параметрів поля випромінювання.*

Як правило, в подібних переносних оперативних системах радіопеленгації використовують фазовані антенні системи (ґратки), які здатні за допомогою електронного керування формувати в дальній зоні відповідні стандартні радіопеленгаційні діаграми спрямованості (РДС). Використання сучасних фазованих антен та антенних систем у нових конструкціях малогабаритних радіопеленгаційних систем UNF діапазону в багатьох випадках не тільки малоефективне, а іноді просто є неможливим, внаслідок існування відомих недоліків, а саме:

- значних габаритів та ваги, що суттєво знижують фактор таємності при проведенні оперативних завдань;
- залежність якості пошуку від тривалості проведення пошукових робіт та метеорологічних обставин;
- значна вартість фазованих решіток.

На рисунку показана спеціальна широкосмугова антена з робочою смугою частот, здатною перекрити фактично всю стандартну смугу частот UNF діапазону. В основу такої антени покладено можливість зміни або регулювання кроку між витками S в просторовій нерегулярній однозаходній дротовій спіральній структурі, що призводить до ефективної зміни характеристик та параметрів поля випромінювання, тобто з'являється можливість формування необхідної діаграми спрямованості спіральної антени (ДСА), в тому числі і трьох відомих класичних радіопеленгаційних діаграм спрямованості (РДС).