РЕФЕРАТ

Звіт по курсовому проекту: 22 ст., 3 рис., 7 посилань, 3 додатків.

Об'єкт дослідження на якому створюється система ТЗІ це 3 кімната на другому поверсі двоповерхової будівлі, далі «кімната для нарад №3». Ця кімната використовується для проведення конференцій, семінарів, нарад тощо. ОТЗ, які знаходяться в цій кімнаті це ПЕОМ, принтер, комп’терний проектор, серед ДТЗС слід виділити внутрішню АТС. Форми ІзОД, які циркулюють в цій кімнаті – це мовна та цифрова в АС. Ця кімната входить в межі контрольованої території, яка охоплює також і суміжню з нею кімнату №2.

Організація ЗАТ«Інститут інформаційних технологій» у місті Харкові за родом своєї діяльності повинна створити ОІД для роботи з ІзОД. Для цього треба на основі вимог керівних документів розробити наступні проекти: акт категоріювання, акт обстеження, наказ на контрольовану зону, модель загроз.

КАТЕГОРІЮВАННЯ, ОІД, ПЕОМ, ОТЗ, ДТЗС, ТЗІ, ІзОД, МОДЕЛЬ ЗАГРОЗ, КЗ

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів……5

Вступ……………………………………………………………………………6

1 Акт категоріюванн……………………………………………………….…..8

2. Акт обстеження…………………………………………………………...…11

3. Наказ на контрольовану зону…………………………………………….....14

4. Модель загроз……………………………………………………………......15

Висновки………………………………………………………………………..17

Перелік посилань……………………………………………………………….18

Додатки ...……………………………………………………………………….19

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС - автоматизована система

ДТЗС - допоміжні технічні засоби

ІЗОД - інформація з обмеженим доступом

КСЗІ - комплексна система захисту інформації

ОТЗ - основні технічні засоби

ПЕМВН – побічні електромагнітні випромінювання випромінювання і наводки

ТЗІ - технічний захист інформації

ТКВІ - технічний канал витоку інформації

ВСТУП

технічний захист інформації (ТЗІ) – діяльність, спрямована на:

1. забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;
2. своєчасне виявлення і протидію загрозам безпеці інформації з обмеженим доступом (ІзОД)[1].

Cистема ТЗІ – сукупність суб’єктів, об’єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та їхня матеріально-технічна база.

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС;

Технічне завдання на створення КСЗІ в АС (ТЗ на КСЗІ) є засадничим організаційно-технічним документом для виконання робіт щодо забезпечення захисту інформації в системі.

Технічне завдання на КСЗІ розробляється у разі необхідності розробки або модернізації КСЗІ існуючої (що функціонує) АС. В разі розробки КСЗІ в процесі проектування АС допускається оформлення вимог з захисту інформації в АС у вигляді окремого (часткового) ТЗ, доповнення до загального ТЗ на АС або розділу загального ТЗ на АС.

Технічне завдання на КСЗІ повинно розробляється з урахуванням комплексного підходу до побудови КСЗІ, який передбачає об’єднання в єдину систему всіх необхідних заходів і засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу АС.

В технічному завданні на КСЗІ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її оброблення в обчислювальній системі АС. Додатково треба викласти вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою АС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Перелік вимог з захисту інформації, які включаються в ТЗ на КСЗІ, може бути для кожної конкретної АС як розширений, так і скорочений відносно рекомендованого в даному документі переліку в рамках діючих законодавчих і нормативних документів.

Вимоги повинні передбачати розроблення та використання сучасних ефективних засобів і методів захисту, які дають можливість забезпечити виконання цих вимог з найменшими матеріальними затратами.

Технічне завдання на КСЗІ є одним із обов’язкових засадничих документів під час проведення експертизи АС на відповідність вимогам захищеності інформації.

# АКТ КАТЕГОРІЮВАННЯ

ЗАТ «Інститут інформаційних технологій»

Затверджую Ректор

3.05.07 ЗАТ «Інститут

інформаційних

технологій»

АКТ № 1112

«категоріювання кімнати для нарад №3»

3.05.07 м. Харків

Комісія в складі:

голова Алоян Л. А.- начальник

члени: Акопян Л. І.– нач. РСО

Кусакін В. В. – зам. нач. РСО

Призначена наказом №1 від 13.03.2007 провела категоріювання кімнати для нарад №3.

Категоріювання проводиться у зв’язку з тим, що система ТЗІ для данного ОІД розробляється і впроваджується вперше.

Комісія розглянула та проаналізувала:

-ситуаційний план (додаток А)

-генеральний план (додаток Б)

-схеми електроживлення

-схеми коммунікацій, що мають вихід за межі КЗ

- план розташування ОТЗ та ДТЗС на ОІД (додаток В)

Категоріюванню підлягають об'єкти, в яких обговорюється, мається, пересилається, приймається, перетворюється, накопичується, обробляється, відображається й зберігається (дали - циркулює) інформація з обмеженим доступом (ІзОД).

До об'єктив, що підлягають категорiюванню, відносяться:

- автоматизовані системи (АС) й засоби обчислювальною техніки (ЗОТ), що діють й проектуються;

- технічні засоби, яки призначені для роботи з ІзОД й не відносяться до АС, за винятком тих, що засновані на криптографічних методах захисту;

- приміщення, призначені для проведення нарад, конференцій, обговорень тощо з використанням ІзОД;

- приміщення, в яких розміщені АС, ЗОТ, інші технічні засоби, призначені для роботи з ІзОД, у тому числи й основані на криптографічних методах захисту.

Категоріювання проводиться з метою вживання обґрунтованих заходив щодо технічного захисту ІзОД, яка циркулює на об`єктах, вид витоку каналами побічних електромагнітних випромінювань й наводок, а також акустичних (вiброакустичних) полів.

Комісія постановила:

1. Серед об’єктів на категоріювання слід виділити наступні: ПЕОМ, приміщення, в якому циркулює мовна ІзОД під час нарад, конференцій тощо та приміщення, в якому циркулює мовна ІзОД, під час бесід між співробітниками цього підприємства.
2. В кімнаті для нарад №3 де циркулює така інформація:

2.1 Мовна інформація (під час занять) вголос, під час розмов між співробітниками цього підприємства. Гриф –конфіденційно

2.2 Інформація в ПЕОМ. Гриф обмеження доступу – конфіденційно

1. Першому об’єкту, ПЕОМ, призначити четверту категорію. Другому об’єкту, приміщенню, де циркулює ІзОД під час конференцій, нарад тощо, також призначити четверту категорію. Третьому об’єкту , приміщенню, де циркулює ІзОД під час розмов між співробітниками цього підприємства, теж присвоїти четверту категорію.
2. У наявності всі НД ТЗІ

Додатки:

1. Ситуаційний план (додаток А)
2. Генеральний план (додаток Б)
3. Схеми електроживлення
4. Схеми коммунікацій, що мають вихід за межі КЗ
5. План розташування ОТЗ та ДТЗС на ОІД (додаток В)

Комісія в складі:

голова Алоян Л. А.- начальник

члени: Акопян Л. І.– нач. РСО

Кусакін В. В. – зам. нач. РСО

Кількість примірників - 1

# АКТ ОБСТЕЖЕННЯ

ЗАТ «Інститут інформаційних технологій»

Затверджую Ректор

3.06.07 ЗАТ «Інститут

інформаційних

технологій»

АКТ № 102

«про обстеження кімнати для нарад №3»

3.06.07 м. Харків

Комісія в складі:

голова Алоян Л. А.- начальник

члени: Акопян Л. І.– нач. РСО

Кусакін В. В. – зам. нач. РСО

Призначена наказом №1 від 13.03.2007 провела обстеження кімнати для нарад №3.

Обстеження проводиться у зв’язку з тим, що КСЗІ для данного ОІД розробляється і впроваджується вперше. Цей документ розробляється виходячи з акту № 1112 «категоріювання кімнати для нарад №3» від 3.05.07, керівник – Ректор.

Комісія розглянула та проаналізувала:

-ситуаційний план (додаток А)

-генеральний план (додаток Б)

-схеми електроживлення

-схеми коммунікацій, що мають вихід за межі КЗ

- план розташування ОТЗ та ДТЗС на ОІД (додаток В)

-наявність НД ТЗІ

Комісія постановила:

1. В кімнаті для нарад №3 де циркулює така інформація:
   1. Мовна інформація (під час занять) вголос та під час розмов між співробітниками цього підприємства. Гриф –конфіденційно
   2. Інформація в ПЕОМ. Гриф обмеження доступу – конфіденційно
2. Відстань до меж контрольованої зони
3. Трансформаторна підстанція, служби, ТП-10/0,4 – за межами контрольованої зони, сторонні споживачі наявні
4. Комунікації виходять за межі контрольованої зони
5. Система заземлення – виходить за межі контрольованої зони (Схеми комунікацій, що мають вихід за межі КЗ)
6. У наявності всі НД ТЗІ

Висновки:

1. Захищаєма мовна інформація не відповідає НД.
2. Захищаєма інформація в ЕОМ не відповідає НД.

Рекомендації:

1. Розробити модель загроз інформації з обмеженим доступом
2. Згідно з моделлю загроз перекривати технічні канали витоку мовної інформації під час нарад та під час розмов між співробітниками цього підприємства
3. Захистити ЕОМ
4. Згідно з моделлю загроз перекривати технічні канали витоку інформації з ЕОМ

Додатки:

1. Ситуаційний план (додаток А)
2. Генеральний план (додаток Б)
3. Схеми електроживлення
4. Схеми комунікацій, що мають вихід за межі КЗ
5. План розташування ОТЗ та ДТЗС на ОІД (додаток В)

Комісія в складі:

голова Алоян Л. А.- начальник

члени: Акопян Л. І.– нач. РСО

Кусакін В. В. – зам. нач. РСО

Кількість примірників - 1

3 НАКАЗ НА КОНТРОЛЬОВАНУ ЗОНУ

ЗАТ «Інститут інформаційних технологій»

Наказ

на контрольовану зону

№541

* + 1. м. Харків

«про призначення контрольованої зони в межах кімнати для нарад №3 та суміжною з нею кімнатою №2»

Причиною для створення цього документу послужило те, що система ТЗІ для даного ОІД «кімнати для нарад №3» розробляється і впроваджується вперше. Цей документ є необхідним для створення системи ТЗІ на ОІД «кімната для нарад № 3».

Цей наказ розробляється виходячи з акту № 1112 «категоріювання кімнати для нарад №3» від 3.05.07, керівник – Ректор та акту №102 «про обстеження кімнати для нарад №3» від 3.06.07, керівник – Ректор.

НАКАЗУЮ:

1 Встановити контрольовану території в межах ОІД «кімнати для нарад №3» та суміжною з нею кімнатою №2.

2 Відповідальним за створення контрольованої території призначити начальника групи ТЗІ Іванова П. П.

Директор Сидоров І. В

Наказ довести начальнику групи ТЗІ Іванова П. П

4 МОДЕЛЬ ЗАГРОЗ

На основі наступних документів: ситуаційний план (додаток А), генеральний план(додаток Б), план розміщення ОТЗ та ДТЗС(додаток В) та план електроживлення ОІД «кімната для нарад №3» була зроблена наступна модель загроз. Носіями ІзОД на даному ОІД можуть бути як акустичні так і цифрові сигнали в АС. Розвідка може вестися як і з позицій зацікавлених сторін вказаних на ситуаційному плані(додаток А), так і з сусідніх кімнат та з нижнього поверху. Джерелом небезпечного сигналу може бути як АС та її компоненти, так і мовна інформація. Розробимо модель загроз для кожного з цих джерел.

1). АС та її компоненти, зокрема монітор, проектор, принтер. Параметри монітора ПЕОМ: r1 = 0,3; r2 = 33. Проаналізувавши план розміщення ОТЗ та ДТЗС(додаток В) зазначаємо, що випадковими антенами в даному приміщені можуть бути система опалення, система сигналізації, система кондиціонування та система електроживлення. Всі ці системи мають вихід за межі контрольованої території і тому їх слід розглядати як можливий канал витоку ІзОД. Для зняття ектричних напруг, струмів з ІзОД на виході цих систем зацікавлена сторона може застосувати чутливий підсилювач. Для уникнення цього можна запропонувати розмістити ПЕОМ від всіх випадкових антен на відстань, яка перевищує r1, тоді рівень небезпечного сигналу буде меншим. Також можна застосувати екранування кабелів ПЕОМ та роздільне прокладання кабелів ОТЗ, ТЗПІ та ДТЗС. Ще можна запропонувати встановити фільтри та екранувати приміщення.

2). Мовна інформація, яка циркулює в даному приміщені є джерелом небезпечного сигналу.

Для здобуття цієї інформації зацікавлена сторона може застосувати:

а). Лазерне опромінення шибок. Для протдії цьому можна запропонувати використовувати генератори просторового зашумлення. б.) Розвідка спрямованим мікрофоном з чутливим підсилювачем. Також можна запропонувати встановити генератори просторового зашумлення та генератори лінійного зашумлення.

в). Розвідка мовної інформації за допомогою підкладних пристроїв. Для уникнення цього можна запропонувати організаційні заходи. Наприклад, частіше робити обстеження кімнати на наявність цих приладів та перевірка всіх відвідувачів цієї кімнати.

3). Акустоелектричні перетворення, які можуть виникнути при попаданні небезпечного сигналу на внутрішню АТС та згодом вийти за межі виділеного приміщення. Ці сигнали можуть бути здобуті зацікавленою стороною за допомогою чутливих підсилювачів. Для протидії цьому можна запропонувати екранувати ДТЗС чи встановити фільтри на комунікації, що мають вихід за межі КЗ.

4). Зацікавлена сторона також може застосувати спеціальний вплив на носії ІзОД і засоби забезпечення ТЗІ шляхом полів, сигналів, що використовуються в технічних засобах забезпечення діяльності, з метою зниження ефектив­ності функціонування системи захисту інформації, створення технічних ка­налів витоку, порушення цілісності інформації (модифікації, руйнування, знищення). Для протидії цьому слід використовувати встановити перешкодозахисні фільтри у колах живлення та у колах комунікацій.

ВИСНОВКИ

Проаналізувавши ситуаційний план(додаток А), генеральний план(додаток Б), план розміщення ОТЗ та ДТЗС(додаток В) та план комунікацій, що мають вихід за межі КЗ були розроблені наступні документи: акт категоріювання, акт обстеження, наказ на контрольовану зону. В акті на категоріювання були визначені об’єкти, які підлягають категоріювання і кожний з них був занесений до окремої категорії, в залежності від рівня ІзОД, яка в ньому циркулює. В аті обстеження були проаналізовані види сигналів ІзОД, які циркулюють в даному приміщені і були зроблені висновки стосовно того, чи відповідає приміщення нормам нормативних документів для приміщень де циркулює ІзОД. В наказі на контрольовану зону були визначені межі контрольованої зони та призначені відповідальні за створення цієї контрольованої зони. На основі всіх цих документів була розроблена модель загроз, де було показано, які існують канали витоку ІзОД з даного приміщення, які можуть бути застосовані засоби зацікавленою стороною для зняття цієї інформації. Після цього для кожного каналу витоку інформації було запропоновані можливі варіанти захисту. По результатам виконаної роботи була створена система ТЗІ для ОІД «кімната для нарад №3».

ПЕРЕЛІК ПОСИЛАНЬ

1. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно – телекомунікаційній системі. НД – ТЗІ 3.7-003-2005.

2. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами ПЕМВН. (ТР ЕОТ-95).

3. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ-ПЕМВН-95).

4. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

6. Конспект лекцій.

7. Методічні вказівки з курсового проектування з ТЗІ.

3 – виділена кімната. ОІД «кімната для нарад №3»

Додаток В ПЛАН РОЗТАШУВАННЯ ОТЗ ТА ДТЗС НА ОІД

ПЕОМ

Комп’терний проектор

принтер

АТС

Пожежна

сиг-ція

Система

опалення

Система

опалення

Схема

електроживлення

Система

кондиціонування



Пояснення до плану розташування отз та дтзс на оід:

Система опалення, схеми електроживлення, система кондиціонування та пожежна сигналізація мають вихід за межі виділеного приміщенн