ПІДВИЩЕННЯ ЗАХИСТУ СИСТЕМИ ГОЛОСУВАННЯ ЗАЛУ ЗАСІДАНЬ З ВИКОРИСТАННЯМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Ілюстративний матеріал
до магістерської кваліфікаційної роботи
За спеціальністю 8.17010301 – «Управління інформаційною безпекою»
08-42.МКР.002.95.000.

Виконала: ст. гр. УБ-15м Каменчук О.О.
Керівник: проф., д.т.н. Яремчук Ю.Є.

АКТУАЛЬНІСТЬ

Захист інформації може бути досягнуто шляхом створення системи захисту інформації на основі комплексного підходу з використання біометричної ідентифікації.

Актуальність полягає в створені комплексної системи захисту інформації, яка буде охоплювати усі можливі загрози з узгодженням між собою різнорідних методів і засобів.

МЕТА І ЗАДАЧІ

Метою магістерської кваліфікаційної роботи є забезпечення захисту системи голосування зали засідань, що буде охоплювати захист інформації від усіх можливих загроз.

Для досягнення цієї мети необхідно дослідити та вирішити такі задачі:

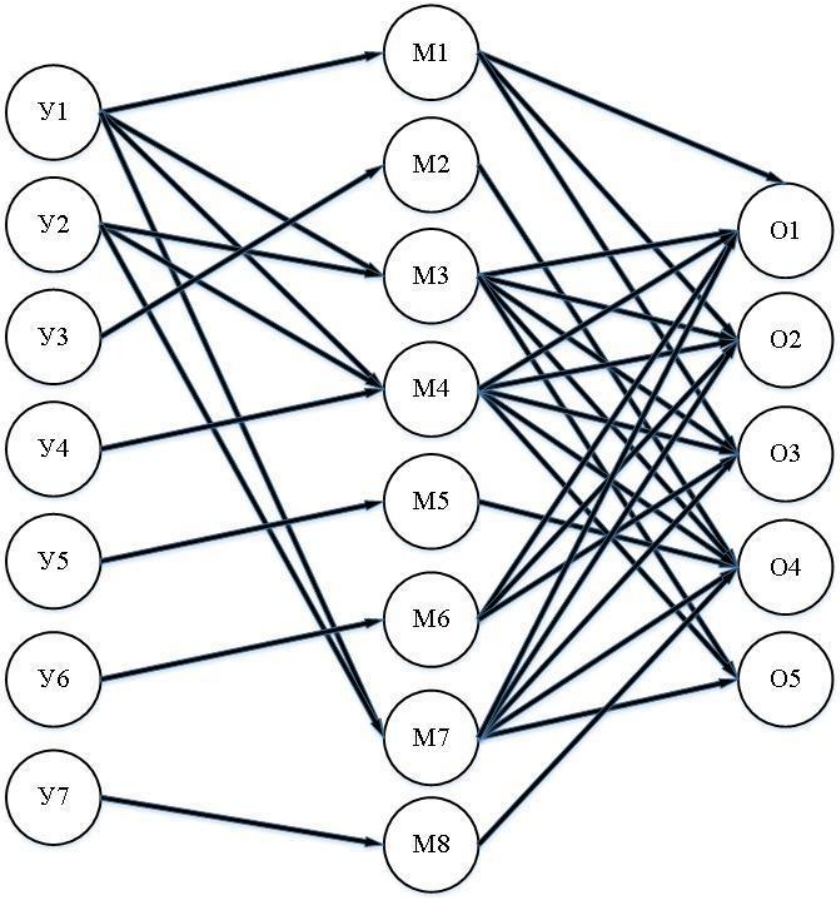
- проаналізувати та дослідити усі можливі системи голосування та їх захист;
- проаналізувати та дослідити ОІД;
- забезпечити захист голосування з використанням біометричної ідентифікації;
- розрахувати економічні показники та термін окупності системи.

МОДЕЛЬ ЗАГРОЗ

В даному випадку потенційними загрозами можуть бути:

- несанкціонований доступ (НСД) за допомогою проникнення зловмисника в приміщення;
- витік інформації за рахунок випадкових чи навмисних неправомірних дій особи, яка має доступ до приміщення;
- витік інформації по вібраційним каналам;
- витік інформації каналами ПЕМВН;
- витік інформації через стільниковий зв’язок;
- витік інформації акустичним каналом.

МОДЕЛЬ ЗАГРОЗ У ВИГЛЯДІ ТРИДОЛЬНОГО ГРАФУ



У – множина загроз інформаційним ресурсам

1 – несанкціонований доступ до інформації
2 – витік інформації за рахунок випадкових чи навмисних дій особи, яка має доступ до приміщення
3 – витік інформації по вібраційним каналам
4 – знімання інформації за допомогою закладних пристроїв, диктофонів
5 – втрата інформації через стільниковий зв'язок
6 – витік інформації каналами ПЕВМН
7 – перехоплення акустичної інформації

М – засоби і заходи щодо захисту інформації

1 – встановлення системи «ЛОЗА-2»
2 – встановлення генератора шумових сигналів «МАРС-ТЗО-4-2»
3 – встановлення системи відеоспостереження
4 – встановлення системи контролю доступом до приміщення
5 – здавання мобільних телефонів перед переговорами
6 – встановлення засобу активного захисту «DELTA-7»
7 – встановлення датчиків руху, відкриття дверей та розбиття скла
8 – встановлення захисних ролет

О – множина об'єктів захисту інформації

1 – бази даних
2 – інформаційні структури, представлені у вигляді окремих файлів
3 – персональні дані
4 – інформація, що озвучується
5 – захищене приміщення

РОЗРОБКА ТЕХНІЧНИХ ЗАХОДІВ

Для забезпечення секретності переговорів перед проведенням нарад слід провести такі технічні заходи:

- перевірка радіоефіру;
- візуальне обстеження приміщення, всіх меблів та інших предметів;
- перевірка приміщення радіолокатором;
- перевірка електротехніки;
- перевірка ліній (телефонної, електричної).

РОЗРОБКА ТА РЕАЛІЗАЦІЯ ПЛАНУ ТЗІ ПО ВПРОВАДЖЕННЮ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ЗАЛИ ЗАСІДАНЬ

Для вторгнення в зал засідань порушник може використовувати апаратні, програмні та спеціальні засоби. Тому необхідно розробити комплексну систему захисту інформації, яка складається з:

- захисту від витоку вібраційним каналом;
- захисту від витоку оптичним каналом;
- захисту від витоку каналами ПЕМВН;
- захисту від НСД;
- система контролю і управління доступом на об’єкті;
- система охоронного телебачення (відеоспостереження);
- система охорони периметра.

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Для захисту голосування було використано біометричну ідентифікацію у вигляді дактилоскопічного сканера, який буде встановлено на кожний із пультів для голосування. Саме такий спосіб голосування дозволить захистити результати голосування та зберегти їхню достовірність.

ІСНУЮЧІ ВИДИ СКАНЕРІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

РОЗРОБКА ОРГАНІЗАЦІЙНИХ ЗАХОДІВ

До організаційних заходів можна віднести:

- обмеження доступу до приміщення сторонніх осіб;
- проведення категоріювання та призначення приміщенню та ІТС певну категорію;
- перед початком переговорів усі учасники здають мобільні телефони;
- створення служби захисту інформації;
- налаштування системи, обробку інформації можуть здійснювати лише адміністратори системи.

ВИСНОВКИ

Під час виконання дипломної роботи було виконано поставлені задачі, а саме:

- досліджено усі існуючі системи голосування та їх захист;
- досліджено об’єкт інформаційної діяльності;
- забезпечено захист системи голосування з використанням біометричної ідентифікації;
- розраховано економічні показники та термін окупності розробленої системи.

В результаті отримано повністю роботоздатну комплексну систему захисту зали засідань, яка складається з багатьох елементів захисту, забезпечує максимально просте керування даним комплексом. Програма захисту голосування на основі біометричної ідентифікації цілком захищає інформацію від витоку та зберігає її достовірність.

ДЯКУЮ ЗА УВАГУ