Звіришин В. М.,
здобувач вищої освіти спеціальності 122 Комп'ютерні науки
Науковий керівник: **Мальченко П. О.,**
асистент кафедри економічної кібернетики,
комп'ютерних наук та інформаційних технологій,
Миколаївський національний аграрний університет, м. Миколаїв

ДЖЕРЕЛА ВИНИКНЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЧЕРЕЗ АУДІО ТА ВІДЕО КАНАЛИ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

У випадках, коли необхідне аудіо- та відеоспостереження приміщень, особливо за відсутності зловмисника, зазвичай використовують вбудовані пристрої або "жучки". У приміщеннях інформаційних систем пристрої для підслуховування зазвичай використовуються для прихованого прослуховування.

Згідно з вітчизняним законодавством, пристрої для підслуховування класифікуються як спеціальні технічні засоби негласного отримання інформації. Ці пристрої поділяються на кондуктивні та випромінюючі. Кондуктивні закладні пристрої вимагають значного часу на встановлення і можуть мати певні індикатори, що свідчать про їхню присутність [1].

Випромінюючі закладки, також відомі як "радіозакладки", швидко встановлюються і можуть працювати автономно протягом тривалого часу завдяки внутрішнім батареям. Однак вони також мають демаскувальну властивість - випромінюють випромінювання в радіо- або оптичному діапазоні. Крім того, радіозакладки можуть слугувати джерелом живлення електричних або акустичних сигнальних мереж, таких як телефонний та гучномовний зв'язок, які самі можуть бути джерелом перехопленої інформації.

Широко використовуються акустичні "радіозакладки", здатні виявляти акустичні хвилі і перетворювати їх в електричні сигнали, що передаються радіохвилями на відстані до 8 км.

Однак на практиці більшість радіозакладок призначені для роботи в діапазоні від 50 до 800 метрів.

Підслуховування більше не потребує фізичного доступу до приміщення. Сучасні технічні засоби дозволяють перехоплювати розмови на відстані кількох сотень метрів. У міських умовах ефективна дальність дії цих пристроїв може зменшитися до десятків метрів під впливом рівня навколишнього шуму.

За допомогою спеціальних пристроїв, що кріпляться на віконні шибки, механічні коливання, викликані акустичними хвилями в приміщенні, вловлюються і перетворюються на електричні сигнали. Ці сигнали передаються радіоканалом на значні відстані.

Ще одним методом отримання аудіоінформації є високочастотне накладання. Цей метод передбачає вплив на елементи, здатні модулювати електромагнітні поля або електричні сигнали, високочастотними сигналами, що містять мовну інформацію. Модуляція - електротехнічний термін, що означає

зміну характеристики сигналу, наприклад, його амплітуди, відповідно до корисного сигналу, в тому числі звукових хвиль.

Такими елементами можуть слугувати різні порожнини з електропровідними поверхнями, наприклад, сейфи або металеві шафи. По суті, вони діють як великі високочастотні контури, що нагадують котушки індуктивності з розподіленими параметрами, які змінюються під впливом акустичних хвиль. Коли частота такого контуру збігається з частотою високочастотного накладання і акустичні хвилі потрапляють на поверхню порожнини, контур повторно випромінює і модулює зовнішнє поле, в результаті чого виникає високочастотний електричний сигнал.

Відеорозвідка слугує методом виявлення та локалізації елементів системи безпеки на об’єктах інформаційної діяльності та розуміння їхніх операційних характеристик. У комп’ютерних системах інформація може бути отримана шляхом візуальної зйомки екранів моніторів і табло через прозорі вікна, якщо відсутні заходи безпеки для протидії таким загрозам.

Цей вид розвідки може проводитися за допомогою різних технічних засобів, включаючи оптичні прилади, фото-, кіно- і телевізійну апаратуру. Багато з цих пристроїв дозволяють зберігати і передавати відеоінформацію на певні відстані. В рамках цієї роботи було проведено дослідження аудиторії вищого навчального закладу.

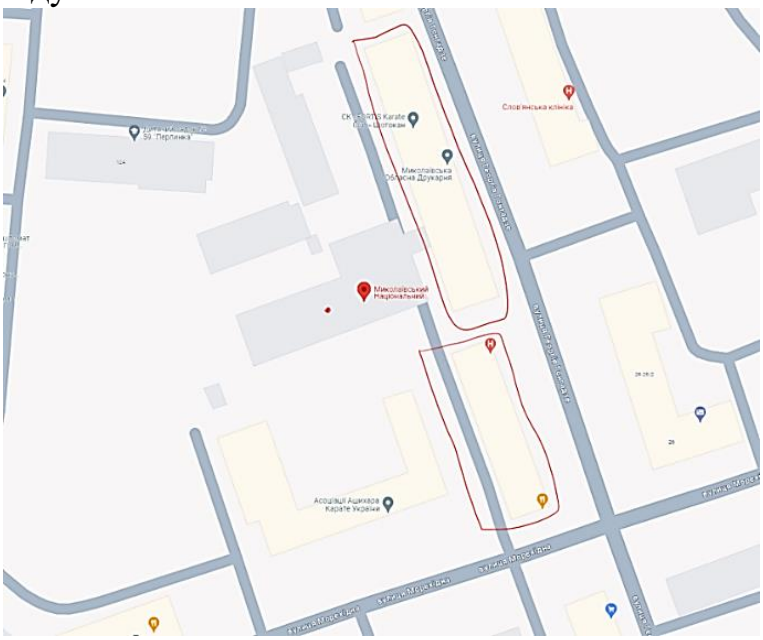

Рис. 1. Ситуаційний план ОІД

Точкою відмічено положення аудиторії. З огляду на червоний контур, можна побачити, що джерелом небезпеки може бути Обласна Друкарня, медичний центр або провулок за ним, де може бути розміщено АЗ для витоку інформації.

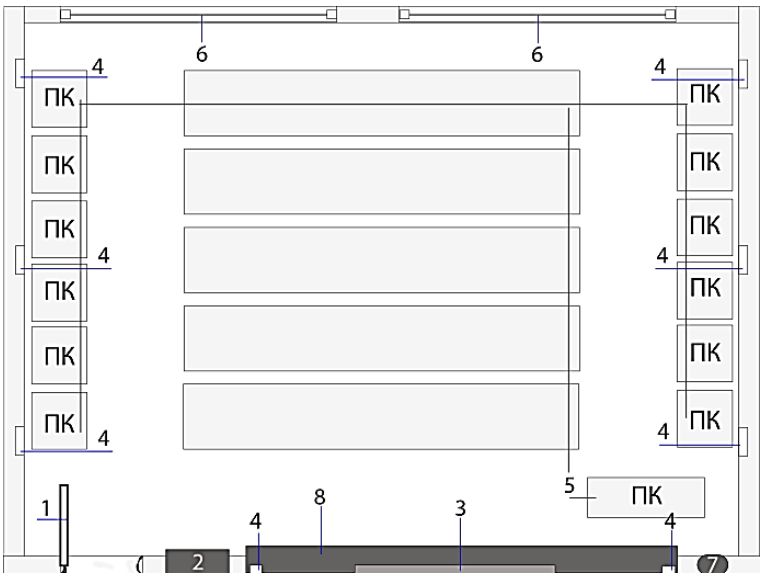

Рис. 2. Генеральний план ОІД

Умовні позначення: 1 – двері; 2 – щит електричний з 3 автоматами; 3 – телевізор; 4 – розетка(и); 5 – стіл(столи) з ПК; 6 – вікно з вертикальними шторами; 7 – система відеоспостереження; 8 – дошка;

Згідно з вказаним планом, наявність камери відеосостереження у приміщенні сприяє забезпеченню безпеки але може допомогти в здійсненні візуального спостереження за подіями в приміщенні при перехопленні доступу до камери, автомат на вході мережі є безпечним засобом від витоку інформації через розетки, хоча таку ймовірність відкидати неможливо. У той же час, відсутність вентиляції унеможливлює розміщення засобів спостереження у складнодоступних місцях. Вікна забезпечені досить ефективною звукоізоляцією, але двері та стіни не можуть впоратися з цією задачею на задовільному рівні.

Список використаних джерел

1. Методологія захисту інформації. Аспекти кібербезпеки: підручник / Г.М. Гулак. К.: Видавництво НА СБ України, 2020, 256 с.