УДК 519.2

Г.О. Димова, І.О. Рудич
Херсонський державний аграрно-економічний університет
anndymova@gmail.com

АНАЛІЗ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ПРОНИКНЕННЯ ДО ОБ'ЄКТУ ЗАХИСТУ

В статті розглянуті основні критерії оцінки ефективності для досягнення оптимізації структури та алгоритмів роботи засобів виявлення несанкціонованого проникнення до об'єкту захисту і запропонована структуризація зон виявлення порушника.

Ключові слова: СИСТЕМА ФІЗИЧНОГО ЗАХИСТУ, ЗАСОБИ ВИЯВЛЕННЯ, НЕСАНКЦІОНОВАНЕ ПРОНИКНЕННЯ, ПОРУШНИК, ДІАГРАМА СПЯМОВАНОСТІ.

The article discusses the main criteria for evaluating the effectiveness to achieve the optimization of the structure and algorithms of the detection of unauthorized penetration of the object of protection and the proposed structuring of zones of detection of the intruder.

Keyworks: PHYSICAL PROTECTION SYSTEM, DETECTION MEANS, UNAUTHORIZED ENTRY, VIOLATOR, RADIATION PATTERN.

Вступ (постановка проблеми). Питання забезпечення безпеки різних об'єктів, в першу чергу, таких як критичної інфраструктури, інформатизації (якими в даний час, по суті, є переважна більшість об'єктів) і т.п. є дуже важливими. Один з найважливіших елементів практично будь-якої системи безпеки (інформаційної, антитерористичної, протикримінальної і ін.) – це система фізичного захисту (СФЗ).

Аналіз останніх досліджень та публікацій. Для виявлення несанкціонованого проникнення (НП) порушника, як однієї з основних загроз, зазвичай використовують системи охоронної сигналізації, як одну з важливих складових СФЗ [1, 2]. При їх розробці та аналізі ефективності першочерговим є досягнення необхідної ефективності виявлення НП. При вирішенні цієї задачі необхідно враховувати не тільки особливості вибору типу і місць установки засобів виявлення (ЗВ), а й можливі методи впливу на ЗВ СФЗ кваліфікованого порушника, що володіє апріорними знаннями про принципи функціонування і параметрах, які використовуються ЗВ. В такому випадку засіб виявлення, що володіє високою надійністю виявлення в стандартних умовах, не зможе виявити кваліфікованого порушника. Тому важливу роль відіграє можливість отримання об'єктивної оцінки ефективності функціонування ЗВ при тих чи інших видах дій порушника. Це дозволить, по-перше, розробляти більш ефективні СФЗ, по-друге, мати можливість оцінки ефективності існуючих систем і, нарешті, здійснювати об'єктивне порівняння різних систем і різних типів ЗВ.

Постановка задачі. Вибір об'єктивних критеріїв оцінки ефективності, справедливих для різних типів засобів виявлення і різних умов.

Основна частина (розв'язання задачі). Основними критеріями оцінки ефективності для оптимізації структури та алгоритмів роботи засобів виявлення несанкціонованого проникнення для даної задачі можуть служити, перш за все, досягнення необхідної ймовірності виявлення $P_{об}$, а також низької імовірності помилкової тривоги $P_{лт}$ і захищеності ЗВ, тобто здатності зберігати свої характеристики при тих чи інших прийомах, що застосовуються порушником для подолання системи охоронної сигналізації.

Однак вимоги до реалізації бажаних значень $P_{об}$ і $P_{лт}$ суперечливі, оскільки збільшення ймовірності виявлення пов'язано з необхідністю підвищення чутливості, в свою чергу, призводить до збільшення ймовірності помилкового спрацьовування. І навпаки, зниження ймовірності помилкового спрацьовування веде до необхідності зниження чутливості з відповідним зменшенням імовірності виявлення НП. Як відомо, основне рішення, що дозволяють реалізувати компроміс між можливостями виявлення і помилкової тривоги, досягається шляхом використання комбінованих пристроїв [3].

У загальному випадку ймовірність виявлення буде функцією декількох основних параметрів. До числа найбільш важливих з точки зору розв'язуваної в роботі задачі можна віднести, перш за все, ефективну поверхню, яка відображає/випромінює $G_{эф}$ порушника, швидкість і напрямок руху порушника, яке можна охарактеризувати кутом φ щодо направлення на ЗВ, а також сукупність $\mathbf{O}^i$ контрольованих засобом виявлення параметрів об'єкта. Тоді ймовірність виявлення можна записати як функцію перерахованих вище параметрів $P_{об}\left(G_{эф}, v, \varphi, \mathbf{O}^i\right)$. Ймовірність $P_{лт}$ залежить від вибору параметрів $\mathbf{O}^i$ і наявності сукупності факторів $\mathbf{E}^j$, що подібні по впливу навколишнього середовища [2], як основної причини помилкових тривог. Таким чином, в загальному випадку треба вирішувати задачу вибору характеристик і параметрів ЗВ, а також структури ЗВ для оптимізації $P_{об}$ і $P_{лт}$ за певним критерієм Ψ, наприклад, мінімаксному

$$\Psi\left\{\max\left[P_{об}(G_{эф}, v, \varphi, \mathbf{O}^i)\right], \min\left[P_{лт}(\mathbf{O}^i, \mathbf{E}^j)\right]\right\}. \qquad (1)$$

Як окремий випадок, проте, широко використовуваний на практиці, можна використовувати критерій досягнення необхідного значення ймовірності виявлення при мінімальному рівні помилкових тривог.

Використання критерію (1) не виключає необхідності виконання і критерію несумісності ефективних дій $S_n^{j\,эф}$ на *j*-е СО і $S_l^{k\,эф}$ на *k*-е СО порушником для зниження ймовірності виявлення, запропонований в роботі [4]

$$\bigcup_{n\in N} S_n^{j\,эф} \cap \bigcup_{l\in L} S_l^{k\,эф} = \varnothing, \ \ j \in J, k \in K. \qquad (2)$$

У цьому виразі сукупність ефективних дій порушника $S_n^{j\,эф}$ включає в себе множину $\mathbf{B}^j = [B_1^j, B_2^j, ..., B_M^j]$ з M можливих пасивних способів впливу B_n^j на *j*-е асіб виявлення і сукупність *L* активних способів впливу $\mathbf{A}^j = [A_1^j, A_2^j, ..., A_L^j,]$ на *j*-е ЗВ. Обмежимося випадком врахування впливу чинників навколишнього середовища $\mathbf{E}^j$ і пасивних дій порушника $\mathbf{B}^j$ в силу специфіки застосування активних впливів.

Зауважимо, що виконання критерію (2) потрібно як при розробці самих сповіщувачів, так і при формуванні їх структури на об'єкті. З числа можливих прийомів порушника, що знижують ймовірність виявлення, розглянемо, перш за все, такий найбільш доступний і ефективний спосіб впливу порушника на один з каналів виявлення, як вибір напрямку руху, при якому чутливість одиночних ЗВ або одного з каналів виявлення комбінованих ЗВ мінімальна. Враховуючи обмеження діапазону швидкостей руху можна вважати $v = const$ та $G_{эф} = const$, тоді критерій (1) спрощується і приймає вид

$$\Psi\left\{\left[P_{об}^{зад}(\varphi, \mathbf{O}^i)\right], \min\left[P_{лт}(\mathbf{O}^i, \mathbf{E}^j)\right]\right\} \qquad (3)$$

Облік параметрів v та $G_{эф}$ може бути виконаний аналогічно впливу напрямку руху на підставі даних за тією ж методикою.

Застосування критеріїв (1) і (3) до обраних типів ЗВ вимагає формалізації структури зон виявлення цих коштів. Скористаємося підходом, запропонованим в [5] і заснованим на структуруванні діаграми спрямованості (ДС) на зони, в яких виявлення порушника можливо з різною ймовірністю, а саме зоною впевненого виявлення (ЗВВ), відповідне виявлення з ймовірністю не менше заданої; зона виявлення, в якій ймовірність виявлення менш заданого

рівня і зона невиявлення (ЗНВ), в якій рівень впливу і (або) його тривалість недостатні для прийняття рішення про виявлення. Тоді зона виявлення відповідатиме зоні, в якій виявлення можливо, але з різною ймовірністю, в тому числі нижче заданої. Рис. 1 ілюструє сказане для направлення входу в ДС перпендикулярно її межі, тобто для $\varphi = 0^0$ (в напряму на ЗВ) або для $\varphi = 90^0$ (збоку ДС).

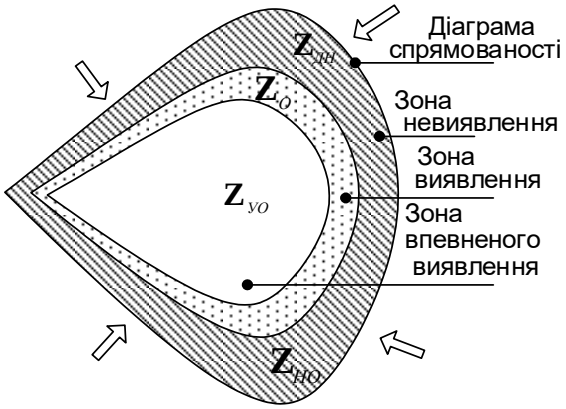

Рис. 1 – Структура діаграми спрямованості

При цьому діаграма спрямованості може бути представлена як множина просторових точок $\mathbf{Z}_{ДН}$, що включає в себе підмножини точок зон $\mathbf{Z}_{УО}$ впевненого виявлення, $\mathbf{Z}_{О}$ виявлення та $\mathbf{Z}_{НО}$ невиявлення $\mathbf{Z}_{ДН} \subset \mathbf{Z}_{УО} \cap \mathbf{Z}_{О} \cap \mathbf{Z}_{НО}$. Очевидно, що множина точок зони впевненого виявлення $\mathbf{Z}_{УО}$ може бути отримана як результат різниці множини $\mathbf{Z}_{ДН}$ і суми підмножин $\mathbf{Z}_{О}$ і $\mathbf{Z}_{НО}$, тобто $\mathbf{Z}_{УО} = \mathbf{Z}_{ДН} \setminus (\mathbf{Z}_{О} \cup \mathbf{Z}_{НО})$.

Основні результати і висновки. Діаграма спрямованості показує можливі способи несанкціонованого проникнення. При цьому необхідно враховувати можливості проникнення як ззовні, так і зсередини ДС. Подальші дослідження спрямовані на оцінку характеру форми і розміру зон впевненого виявлення, виявлення і невиявлення.

ЛІТЕРАТУРА:

1. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
2. Столлингс В. Криптография и защита сетей. М.: Вильямс, 2001. 672с.
3. Волхонский В.В. Извещатели охранной сигнализации. Изд. 4-е доп. и перераб. СПб.: Экополис и культура. 2004. 272 с.
4. Волхонский В.В. К вопросу повышения вероятности обнаружения несанкционированного проникновения на охраняемый объект. *Вестник Воронежского института МВД России*. 2011. №4. С. 37-44.
5. Бендат Дж., Пирсол А. Измерение и анализ случайных процессов. М.: Изд-во «Мир», 1971. 408 с.