УДК 004.056(043.2)
DOI: 10.31673/2409-7292.2020.014248

Лобанчикова Н.М.

МОДЕЛЬ ПОБУДОВИ МОБІЛЬНОЇ СИСТЕМ ОХОРОНИ ПЕРИМЕТРУ ТЕРИТОРІЇ

В статті запропоновано моделі та методи побудови мобільних (швидкого розгортання) систем охорони периметру території, що являє собою інформаційну технологію, що спрямована на підвищення рівня захищеності підрозділів охорони та добуваючих підрозділів шляхом автоматизації процесу виявлення порушників периметру, прийняття управлінських рішень щодо генерації тривоги по підрозділу. Запропоновано структурну модель системи, модель взаємодії компонентів системи.

Ключові слова: периметр, охорона, інформаційна технологія, системи захисту інформації.

Вступ

В сучасних умовах підвищення рівня терористичної діяльності та проведення антитерористичної операції на сході України гостро постає питання охорони периметру мобільного об’єкту при проведенні розвідувальних операцій, перевезенні вантажів, охорони блок-постів. Складність захисту такого роду об’єктів обумовлена використанням в «польових умовах» (енергонезалежність всіх складових системи) та необхідністю адаптування до рельєфу території та інших складових навколишнього середовища (сніг, дощ, мороз, спека, вплив електромагнітного випромінювання). Крім цього, слід додати наступні особливі умови експлуатації, як мінімізація часу на розгортання, відсутність мертвих зон, обмежена кількість персоналу (охоронців), маскування засобів виявлення та стійкість до збурень (грозові розряди, джерела потужних електромагнітних випромінювань), несприйнятливість до зовнішніх чинників “нетривожного” характеру (дрібні тварини, птахи) та стійкість до атак супротивника (злочинця).

Побудова такого роду систем неможлива без використання сучасних інформаційних технологій, досягнень науки та техніки, інноваційних підходів до побудови. Тому розробка вітчизняних моделей, методів та технологій побудови мобільних систем охорони периметру є актуальною науково-технічною задачею сьогодення.

Аналіз існуючих рішень

Вагомий внесок у створення подібних систем та розвиток методів і засобів їх побудови внесли роботи таких вітчизняних та закордонних авторів: Вінцюка Т.К., Шлезінгера М.І., Оленіна Ю.А, Кузнєцова О.О., Юдіна О.К., Корченка О.Г, Конаховича Г.Ф. Новікова О.М., Гайворонського М.В., Шелупанова О.О., Афанасьева О.О., Бурячка В.Л., Толюпи С.В., Козачка В.А., Лукової-Чуйко Н.В., Коцюби В.П., Жукова В.І., Шапиро Л., Уоссермена Ф., Стокмана Дж. та ін.

Аналіз робіт [1-14] вказаних авторів показав, що вони направлені, в основному, на розробку моделей та методів побудови інтелектуальних інформаційних систем виявлення порушника (інцидентів); технічних засобів захисту інформації; систем однофакторної та багатофакторної ідентифікації особи; методів автоматизації обробки зорової інформації; створення засобів фізичного захисту.

Побудова такого роду систем неможлива без використання сучасних інформаційних технологій, досягнень науки та техніки, інноваційних підходів до побудови. Тому розробка вітчизняних моделей, методів та технологій побудови мобільних систем охорони периметру є актуальною науково-технічною задачею сьогодення.

Мета і завдання дослідження. Метою дослідження є вирішення важливої науково-технічної задачі підвищення рівня захисту периметру території від несанкціонованого доступу, суттю якого є аналіз, розробка моделей, методів та технологій побудови мобільних (швидкорозгортаючих) систем охорони периметру для захисту тимчасових об’єктів та інтеграції в комп’ютеризовану систему контролю доступу на об’єкт.

Основними завданнями дослідження є: аналіз засобів виявлення в системах охорони периметру, розробка структурної моделі мобільної системи охорони перимметру, взаємодії компонентів системи.

Основна частина

1. Теоретичні основи побудови

На теперішній час, як вітчизняні, так і закордонні виробники використовують широкий спектр фізичних принципів побудови електронних систем охорони. Найбільш розповсюджені радіохвильові, радіопроменеві, оптичні, ємнісні, вібраційно-чутливі, контактні, сейсмічні, волоконно-оптичні системи та ін., рисунок 1.

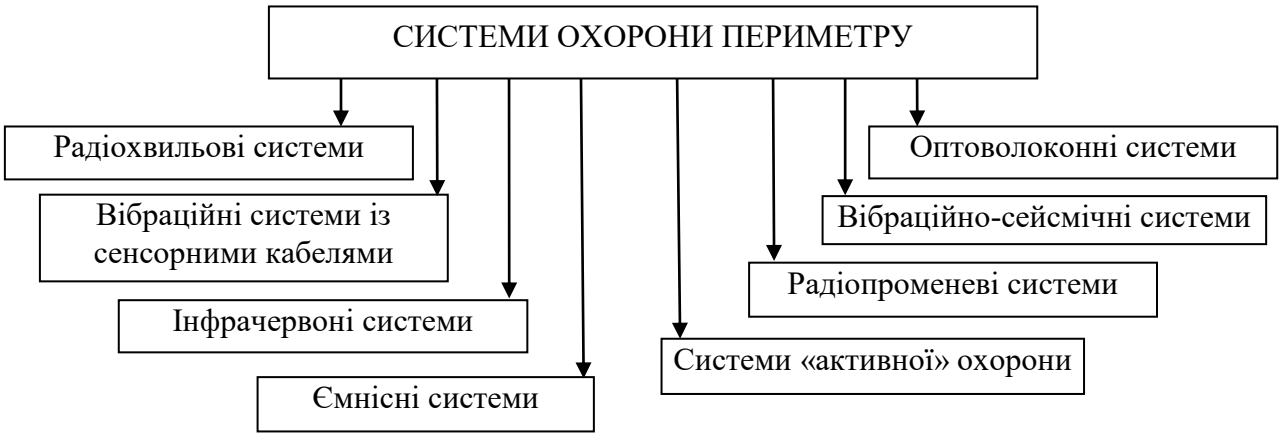

Рис.1. Класифікація систем охорони периметру

Засоби сигналізації призначені для раннього виявлення різноманітних несанкціонованих порушень. Для виявлення факту вторгнення порушника в зону охорони можуть бути використані різні фізичні принципи, що дозволяють з тим або іншим ступенем імовірності розрізнити сигнал спричинений діями порушника, на фоні перешкод різного походження. Класифікація периметрових засобів виявлення (ПЗВ) за їхніми фізичними принципами наведена в структурній схемі (див. рис. 2).

Слід зазначити, що широке використання технічних засобів охорони (ТЗО) дозволяє виключити або звести до мінімуму негативний вплив самої ненадійної ланки в системі охорони – людини. Людині в процесі тривалого чергування властиві стомлюваність, неуважність, навіть недбалість. При цьому, організація охорони за допомогою ТЗО обходиться значно дешевше, а надійність при цьому підвищується.

Тенденції розвитку сучасних периметрових засобів виявлення спрямовані на:

- зниження собівартості датчиків і чутливих елементів;
- підвищення тактико-технічних характеристик;
- підвищення надійності;
- підвищення довговічності;
- зниження частоти помилкових спрацювань;
- підвищення завадостійкості та ін.

В теперішний час здійснюється перехід на цифрову обробку сигналів на основі мікропроцесорної техніки, що забезпечує компенсацію впливу зовнішніх факторів, розпізнавання типових сигналів, автоматичну діагностику і настроювання датчиків під конкретні умови експлуатації. Упровадження цифрових методів обробки дозволяє одержати принципово нові якісні характеристики системи охорони в цілому, забезпечити велику імовірність виявлення на фоні численних зовнішніх і дестабілізуючих факторів, створити клас інтелектуальних датчиків, які самонавчаються, що адаптуються до конкретних умов експлуатації при збереженні високих сигналізаційних характеристик.

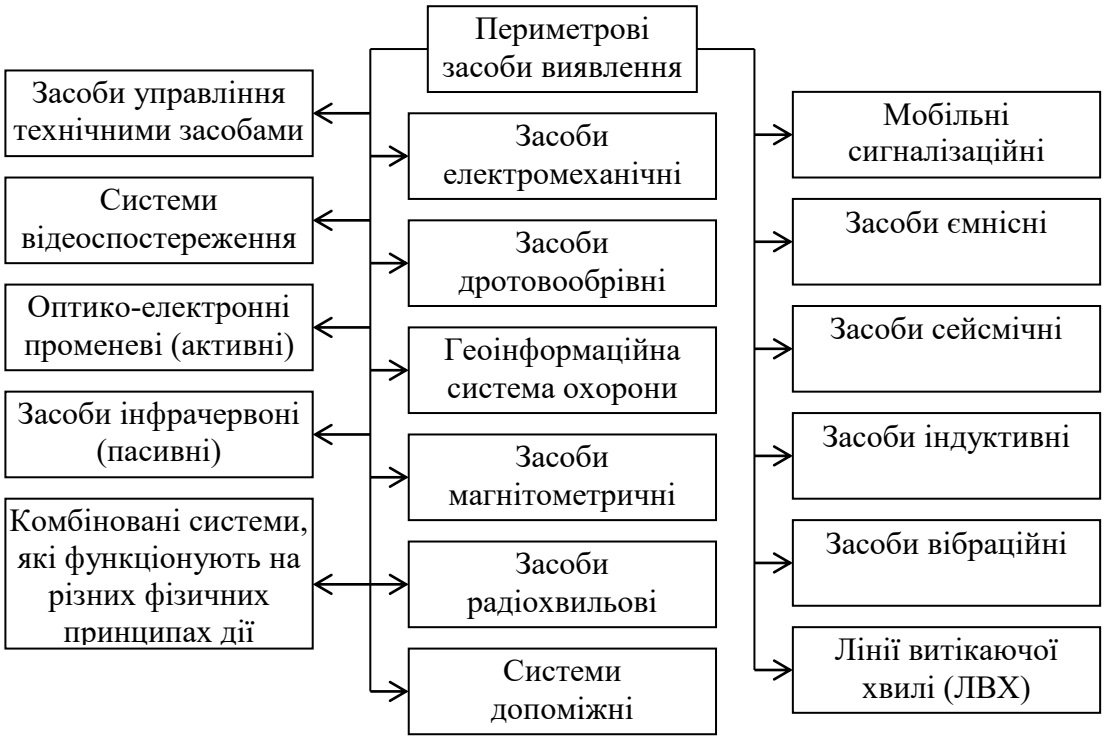

Рис.2. Класифікація периметрових засобів виявлення за їх фізичними принципами дії

В даний час у деяких країнах проводяться розробки мобільних сигналізаційних комплексів. Системи такого типу мають малі габарити, вагу й енергоспоживання, що дозволяє забезпечити приховану і швидку установку на «рубежі» охорони, навіть на непідготовлених в інженерному відношенні ділянках пересічної і лісистої місцевості. Вони можуть застосовуватися на окремих ділянках периметрів об'єктів, обладнаних стаціонарними системами, у період їхнього ремонту або надзвичайних ситуацій. Тактико-економічні характеристики мобільних комплексів, можливість створення на їхній основі систем мобільного захисту (СМЗ) без виконання трудомістких проектних і будівельно-монтажних робіт, а також можливість оперативної зміни, у разі потреби, конфігурації контрольованого рубежу, робить їх привабливими для використання при рішенні задач у системах охорони стаціонарних об'єктів. Це стає можливим при невеликих змінах конструкції їхніх монтажних частин.

Досвід проведення антитерористичної операції на сході нашої країни, участі окремих підрозділів збройних сил України у миротворчих операціях, збройних конфліктах, проведення аналізу діяльності екстремістських організацій проти військових об'єктів показав, що ефективність підготовки військ (сил), збереження життя та здоров'я особового складу, охорона боєприпасів і військової техніки знаходяться у прямій залежності від якості організації охорони військових об'єктів, а також можливості у автоматичному режимі виявляти порушників на підступах до об'єктів, що охороняються. Обладнання радіоелектронними технічними засобами охорони (ТЗО) ближніх і дальніх підступів до позицій блокпостів, механізованих підрозділів, районів зосередження та розташування бойової техніки, складів дозволить вартам, патрулям, сторожовим постам, спостережним пунктам надійно охороняти військові об'єкти.

Аналіз останніх досліджень [11-13] з питань удосконалення систем технічного захисту військових об'єктів і підступів до них та їх порівняння із аналогічними системами збройних сил найбільш розвинених країн світу свідчить про те, що сучасні принципи організації

системи охорони тимчасово розташованих військових об'єктів (ТРВО), що швидко розгортаються (ШвР), у ЗС України впроваджуються недостатньо ефективно.

В країнах НАТО (насамперед у збройних силах США) обладнання ТЗО ШвР почало розроблятися й застосовуватися ще з 70-х років минулого століття. У Радянському Союзі його розробка почалася в середині 80-х років. З утворенням незалежних держав цьому напрямку досліджень достатньої уваги не приділяється.

Для побудови мереж ТЗО ШвР мобільних об'єктів (літаків, бойової техніки, транспортних засобів) на тимчасових стоянках, а також окремих будинків, внутрішніх приміщеннях складів, ангарів і захищених укриттів застосовуються переносні засоби охорони об'єктів. Найбільш широкого використання в охороні тимчасових і рухливих об'єктів ЗС США одержали переносні РЛС AN/ PPS-5 і -15 різних модифікацій. Патрулі охорони озброюються ручними РЛС (AN/PPS-9, -11, -12, -13, -14). Для охорони тактичних підрозділів сухопутних військ США розроблена легка портативна РЛС OGR (Organic Ground moving target indication Radar), що забезпечує виявлення людей, що рухаються, і транспортних засобів на дальності до 10…20 км в простих і складних метеоумовах. Цю станцію розміщують на автомобілі, що дозволяє організовувати мобільну охорону замість використання для цих цілей переносних РЛСП, протипіхотних і сигнальнобойових мін. Також використовується переносна тактична система охорони OSTSS (Omnisense Tactical Security System), з мініатюрними радіостанціями охорони TSR (Tactical Sentry Radio) та акустична РСП ACVS (Acoustic Cueing and Validation Sensor), що виявляє й класифікує цілі на дальності від 20 до 40 км [11-13]. При необхідності швидкого створення системи охорони тимчасових споруджень і мобільних об'єктів широко застосовуються розвідувально-сигналізаційні системи. Для цих цілей на сьогодні використовують ся системи IREMBASS, PEWS-2, MIDS-EMIDS, REMBASS-2, TRESS, MPNSS та ін. [11-13].

Основним завданням ТЗО для охорони ТРВО повинна бути тимчасова, швидка й надійна організація охорони районів, рубежів, об'єктів, місць дислокації особового складу, бойової техніки, арсеналів зі зброєю, складів, сигналізуючи про вторгнення порушників, диверсантів, злодіїв. Рубежі охорони об'єктів, що охороняються, повинні бути замкнуті, зони виявлення – перекриватися, але на місцевості зі складним, горбкуватим ландшафтом, з лісами та ярами цю вимогу можливо реалізувати тільки частково. Тому в таких районах додатково необхідно використовувати РЛСП і РЛСР наземних цілей, у схованках біля стежок лісових доріг, а в ярах, на гірських перевалах слід закладати дистанційно керовані радіоелектронні (оптичні) засоби виявлення. Такі радіоелектронні системи ТЗО дозволятимуть непомітно виявляти, підраховувати, класифікувати й визначати напрямок пересування живої сили й самохідної техніки, передавати дані на ПКІ по радіоканалу. Передача інформації (сигналів виявлення) від таких ТЗО на ПКІ (віддалених на 10…20 км) повинна здійснюватися по завадозахищеним УКХ радіоканалам.

2. Структурна модель мобільної системи охорони периметру

Проведемо розробку моделі мобільної системи охорони периметру (МСОП), що являє собою автоматизовану інтегровану систему, спрямованау на підвищення рівня захищеності (периметрового захисту) об'єкту охорони, шляхом автоматизації процесу виявлення порушників периметру, прийняття управлінських рішень щодо генерації тривоги по підрозділу.

Поставлена мета досягається синтезом інтегрованих блоків, а саме впровадженням: підсистеми безконтактної радіочастотної ідентифікації (RFID) (Модуль 1); підсистеми інтелектуального відеоспостереження (Модуль 2); СППР із виявлення та попередження НСД на території об'єкту охорони (Модуль 3); підсистеми виявлення руху по контуру периметру захисту (Модуль 4). Структурна схема складових МСОП, спричинених діями особи, представлена на рис. 3.

Основними задачами Модулю 1 (М1) є:

– ідентифікація персоналу на території об'єкту охорони;
– визначення місцезнаходження персоналу на території об'єкту охорони;

– визначення персоналу, що наближається до периметру території об'єкту охорони.

Вихідними даними цього модулю є цифрова комбінація ідентифікатора, яка слугує вхідним потоком для роботи Модулю 3.

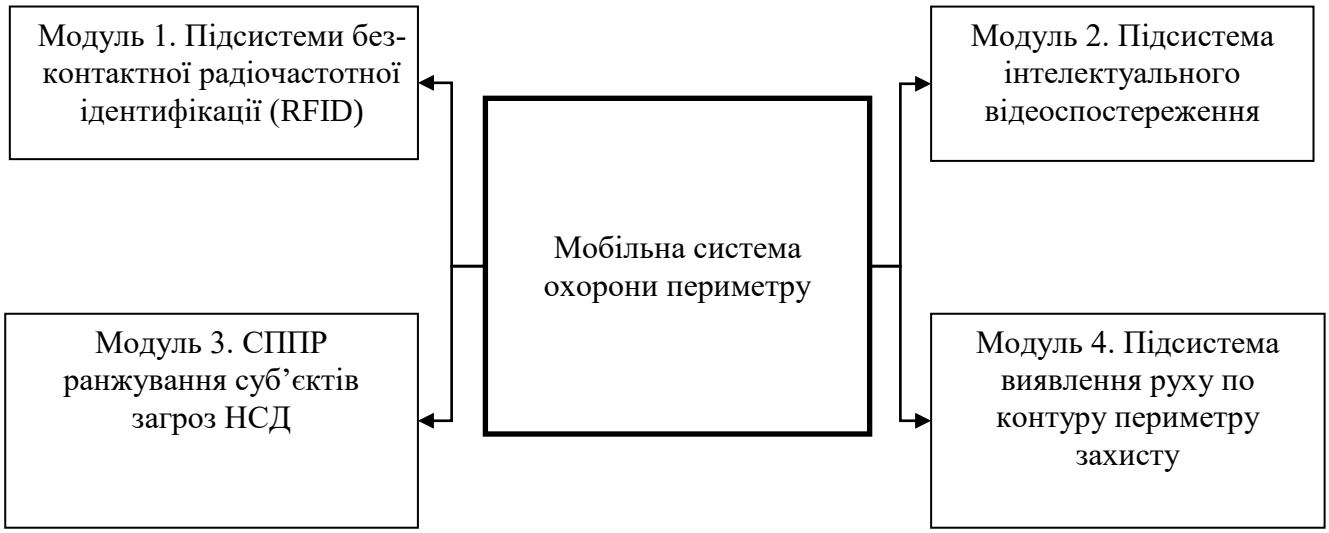

Рис. 3. Структурна схема мобільної системи охорони периметру

До основних задач Модулю 2 (М2) належать:

– ведення відеоспостереження за персоналом на території об'єкту охорони;

– ведення відеоспостереження за периметром території об'єкту охорони;

– надання користувачу інформації про порушника, який потрапив на територію об'єкту охорони;

– передача відеоінформації про НСД користувачу для оперативного прийняття адекватного рішення.

Основними задачами Модулю 3 (М3) є автоматизація процесів прийняття управлінських рішень оператором з:

– виявлення суб'єктів погроз; категоризації суб'єктів погроз за принципом небезпечності;

– визначення категорії небезпеки.

Основною задачею Модулю 4 (М4) є виявлення вторгнення на територію периметру об'єкту охорони.

Модель взаємодії компонентів системи представлена на рис. 4. Вхідними даними системи є $\mathbf{F}=\{F_1,\ldots,Fi\}$ – множина сигналів RFID-міток, що отримані RFID-зчитувачами, $\mathbf{G}=\{G_1,\ldots,G_k\}$ – потік відеоданих, що надходить із відеокамер, $\mathbf{R_{інф}}=\{R_{інф1},\ldots,R_{інфр}\}$ – потік інформації, що надходить від ресурсів захисту території військової частини, $\mathbf{H}=\{H_1\ldots H_y\}$ – множина сигналів від датчиків руху.

Інформаційні потоки для взаємодії системи складають:

– F_{ikod} – цифровий код (ідентифікатор), отриманий від RFID-мітки *i*-го працівника, $i=\overline{1..n}$;

– $\mathbf{G_v}=\{G_{v1},\ldots,G_{vn}\}$ – послідовність оцифрованих кадрів у вигляді зображень у форматі BMP, що надходять від відеокамер;

– $\mathbf{P}=\{P1,\ldots,P\eta\}$ – виявлені суб'єкти погроз;

– $\mathbf{W}=\{W_1,\ldots,W_\lambda\}$ – множина параметрів, що контролюються та аналізуються для визначення категорії небезпеки суб'єктів погроз.

Керуючими впливами виступають: F_{ikodz} – ідентифікатор *i*-ої особи персоналу.

Вихідним параметром системи є інформативний вектор **W***=*{Wi}*, i=1…λ, який передається каналами зв'язку як електронне повідомлення добового наряду об'єкту охорони, і, у разі потреби, до зовнішніх силових структур; інформаційний вектор **D**=*{D_l}, $l=1…\varepsilon$,* генерується системою автоматично та видається черговому добового підрозділу, передається у разі потреби, до зовнішніх силових структур; **R** – рішення СППР із ранжування суб'єктів загроз на території добуваючого підрозділу, **S** – рішення СППР із виявлення НСД суб'єктів загроз на території об'єкту охорони.

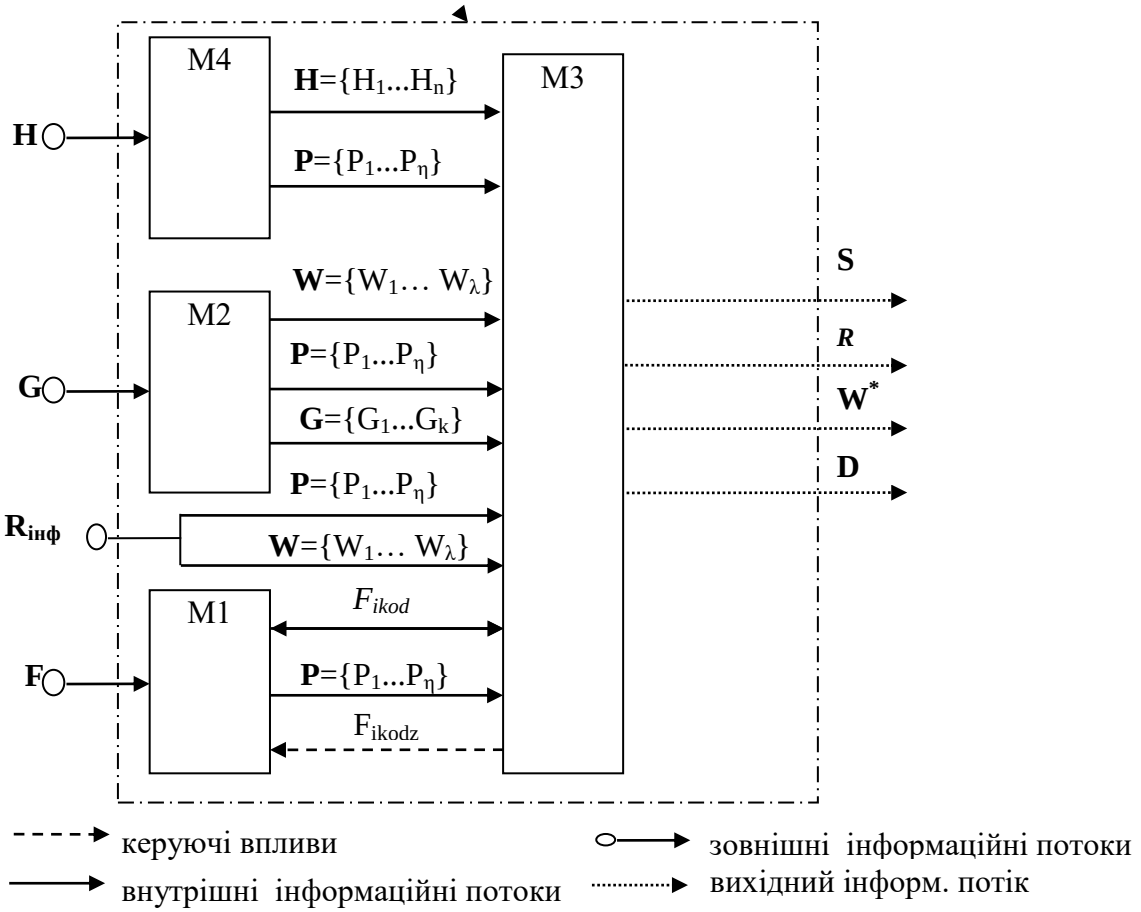

Рис. 4. Модель взаємодії компонентів мобільної системи охорони периметру

Проведемо побудову моделі прояву суб'єктів погроз виникнення НСД. До суб'єктів погроз (Р) відносимо: психічно неврівноважених осіб (P_1); шпигунів (P_2); регіональні терористичні організації (P_3); міжнародні терористичні організації (P_4); екстремістів-одинаків або групи екстремістів (P_5); диверсійно-розвідувальні групи (P_6). Їх можна представити у вигляді відкритого класифікаційного угрупування суб'єктів погроз $\mathbf{P}=\bigcup_{\eta} P_\eta$ (множини суб'єктів погроз), які відповідно до умов експлуатації системи можна доповнювати або адаптувати.

Далі необхідно розробити, модель прояву суб'єктів погроз виникнення НСД на території об'єкту охорони, модель процесу визначення рівня небезпеки суб'єктів погроз виникнення НС на території об'єкту охорони, блок прийняття управлінських рішень.

Висновки

1. В результаті проведеного аналізу фізичних принципів дії засобів виявлення, що використовуються в системах охорони периметру, визначено переваги та недоліки кожного з них, представлено класифікацію систем охорони периметру та класифікацію периметрових засобів виявлення, розглянуті основні типи загороджувальних конструкцій та найбільш відомі системи охорони периметру.

2. Аналіз мобільних засобів охорони дозволив визначити склад, функціональні особливості такого роду систем. Визначено, що для організації охорони тимчасово розташованих об'єктів можливе впровадження двох груп технічних засобів охорони – відповідно рубіжно-сигналізаційних та розвідувально-сигналізаційних.

3. Вперше запропоновано та обґрунтовано структуру складових мобільної системи охорони периметру, яка включає підсистему безконтактної радіочастотної ідентифікації (RFID), підсистему інтелектуального відеоспостереження, СППР із виявлення та попередження НСД на території об'єкту охорони, підсистеми виявлення руху по контуру периметру захисту. Інтеграція та впровадження вказаних підсистем дозволить автоматизувати процес виявлення порушників на підходах до території об'єкту охорони, прийняття управлінського рішень щодо генерації тривоги по підрозділу.

4. Вперше розроблено модель взаємодії компонентів інформаційної системи ранжування суб'єктів загроз несанкціонованого доступу до периметру території об'єкту охорони, яка визначає інформаційні потоки та реалізує взаємодію між компонентами системи. Визначено формальний вигляд інформаційних векторів, що передаються.

Перелік посилань

1. Юдін О. К. Сучасні практики впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури / О. К. Юдін, Р. В. Зюбіна, О. В. Матвійчук-Юдіна // Наукоємні технології. – 2019. – № 1. – С. 36-43.

2. Корченко А.Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с

3. Захист інформації та економічна безпека підприємства: монографія [Текст] / О.О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Харків: Вид. Хнеу, 2008. – 360 с.

4. Грайворонський М.В. Безпека інформаційно-комунікаційних систем [Текст] / М.В. Грайворонський, О.М. Новіков – К.:Видавнича група bhv, 2009.– 608 с.

5. Пількевич І. А. Захист інформації в АСУ : навч. посібник [Текст] / І. А. Пількевич, К. В. Молодецька, Н. М. Лобанчикова. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – 170 с.

6. Кавун, С. В. Інформаційна безпека: підручник / С. В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.

7. Завгородний В. И. Комплексная защита информации в компьютерных системах : учебное пособие [Текст] / В. И. Завгородний. – М. : Логос; Пбоюл, 2001. – 264 с.

8. Белов Е. Основы информационной безопасности : учебное пособие для вузов [Текст] / Белов Е., Лось В., Мещеряков А. – М. : "Студио", 2006. – 356 с.

9. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации: [учеб. пособие для вузов]. – М. : Горячая линия-Телеком, 2004. – 280 с.

10. Згуровський, М.З. Основи системного аналізу: підручник [для студ. вищ. навч. закл.] / М.З. Згуросвський, Н.Д. Панкратова. – К: Видавнича група BHV, 2007. – 544 с.

11. Коцюба В.П. Удосконалення організації охорони тимчасово розташованих військових об'єктів шляхом впровадження сучасних технічних засобів охорони / В.П. Коцюба // Наука і техніка Повітряних Сил : Наук.-техн. журн. – Х.:ХУПС, 2011.– №1(5) – С.164–167.

12. Жуков В.І. Визначення шляхів протидії диверсіям формувань сил спеціальних операцій / В.І.Жуков, В.П. Коцюба, О.С. Тітов // Збірник наукових праць ХУПС. – Х.:ХУПС, 2010. Вип. (4)26. – С. 10-14.

13. Дзеверін І.Г. Синтез структури комплексної системи охорони і оборони військових об'єктів Повітряних Сил / І.Г. Дзеверін І.Л. Костенко, О.М. Борщевський //Наука і техніка Повітряних Сил : Наук.-техн. журн. – Х.:ХУПС, 2010. – Вип. (2)4, – С. 186-190.

14. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А. Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345с.

Надійшла: 22.01.2020 Рецензент: к.т.н., Шуклін Г.В.