УДК 004.932.75:519.76 **Лобанчикова Н.М., Креденцар С.М.**

МОДЕЛЬ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЗАХИСТУ ТЕРИТОРІЇ АЕРОПОРТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Вступ

Зростання актів незаконного втручання в діяльність авіації та нанесення матеріальних, моральних та фізичних збитків авіаційним підприємствам спричинило зростання вимог до оперативності та обґрунтованості управлінських рішень служб безпеки аеропорту щодо виявлення суб'єктів погроз та ліквідації проявів несанкціонованого доступу до території аеропорту.

Таким чином, нагальним є вирішення важливої науково-технічної проблеми, яка пов'язана з підвищенням рівня безпеки аеропортів, суттю якої є розробка комплексних систем захисту території аеропорту від несанкціонованого доступу. Однією із науково-технічних задач постає розробка моделей, методів та засобів побудови автоматизованої системи захисту периметру території аеропорту від несанкціонованого доступу.

Аналіз існуючих рішень. Сьогодні, досить широко представлено ринок «периметрових» систем захисту території об'єктів, але їх поодиноке використання в сучасному терористичному суспільстві є недостатнім, тому з'явилися підходи, методи та засоби побудови комбінованих «периметрових» систем захисту території важливих об'єктів [1], але, нажаль, вони не дають бажаного результату. На сучасному етапі розвитку науки і техніки вагоме місце займають інтелектуальні системи, системи підтримки прийняття управлінських рішень [2-3], сучасні підходи до інформатизації управління регіональною безпекою [4-7]. Запропоновані моделі, методи та засоби створили позитивні передумови для удосконалення систем захисту периметру особливо важливих об'єктів та розроблення наукових підстав побудови автоматизованої системи захисту території аеропорту від несанкціонованого доступу.

Метою даної роботи є розробка структурної моделі, моделі взаємодії компонентів автоматизованої системи захисту території аеропорту від несанкціонованого доступу (АСЗ території аеропорту від НСД), моделі процесу виявлення суб'єктів погроз у зоні загального доступу до території та у контрольованих зонах аеропорту. Основними **завданнями** роботи є: виявлення чинників та їх систематизація для побудови моделі процесу виявлення суб'єктів погроз, визначення потенційних об'єктів ураження та засобів захисту.

Основна частина

Проведений аналіз особливостей функціонування міжнародних аеропортів, методів та засобів побудови систем захисту периметру таких об'єктів, методів та засобів побудови систем підтримки прийняття управлінських рішень [1-7] дозволили виявити наступне: недоліком переважної більшості систем несанкціонованого доступу є направленість на вирішення вузької задачі захисту і відсутність використання комплексного підходу до побудови; відсутність систем підтримки прийняття управлінських рішень операторів служби безпеки; відсутність автоматизованих систем ідентифікації особи з варіюванням декількох біометричних ідентифікаторів.

Нами пропонується модель автоматизованої системи захисту території аеропорту від несанкціонованого доступу, яка представляє собою сукупність математичних моделей і методів, інформаційних і програмно-технічних засобів, взаємопов'язаних і взаємодіючих із користувачами (працівниками служб авіаційної безпеки) при підготовці, прийнятті і контролі виконання управлінських рішень щодо захисту об'єктів ураження від вражаючих впливів внутрішнього та зовнішнього походження.

Поставлена мета досягається синтезом інтегрованих блоків, а саме впровадженням: автоматизованої геоінформаційної системи відображення поточної обстановки на території аеропорту (Модуль 1); підсистеми безконтактної радіочастотної ідентифікації (RFID) (Модуль 2); автоматизованої системи визначення місцезнаходження пасажирів та персоналу на території аеропорту (Модуль 3); СППР із виявлення та попередження суб'єктів погроз на території аеропорту (Модуль 4); підсистеми інтелектуального відеоспостереження (Модуль 5);

автоматизованої системи ідентифікації особистості (Модуль 6). Структурна схема складових системи представлена на рис. 1.

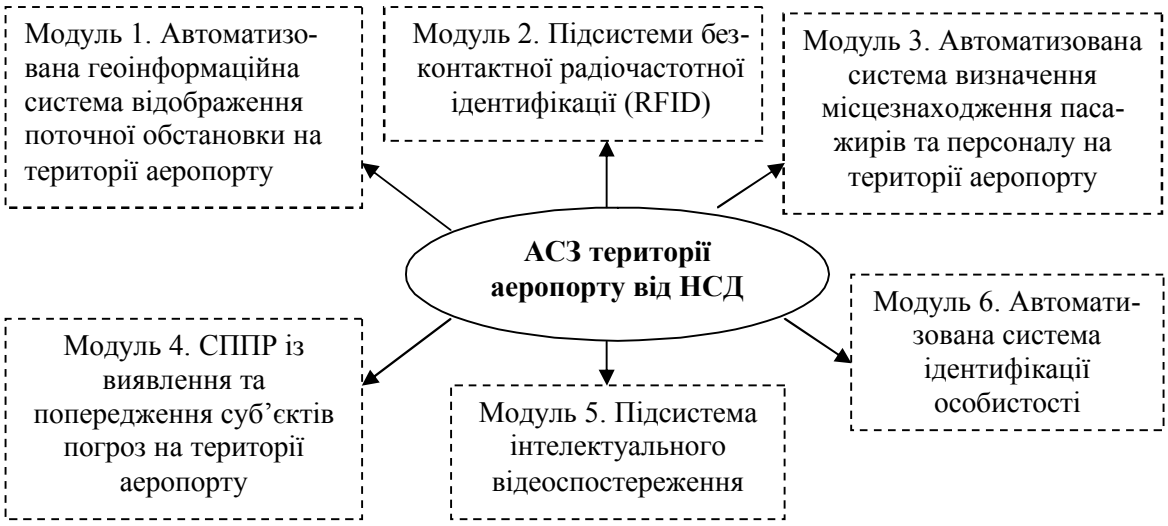

Рис. 1. Структура АСЗ території аеропорту від НСД

Модель взаємодії компонентів АСЗ території аеропорту від НСД представлена на рис. 2. Вхідними даними системи є $\mathbf{F}=\{F_{1,\dots,}F_n\}$ – множина сигналів RFID-міток, що отримані RFID-зчитувачами, $\mathbf{G}=\{G_1,\dots,G_n\}$ – потік відеоданих, що надходить із відеокамер, $\mathbf{I^{vh}}=\left\{I_1^{vh},\dots,I_n^{vh}\right\}$ – послідовність звукових файлів *i*-го мовця типу WAV, формату RIFF, що отримані мікрофонами на входах у контрольовані зони аеропорту, $\mathbf{P_{pv}}=\{P_{pv1},\dots,P_{pvn}\}$ – послідовність зображень папілярного відбитку *i*-го працівника чи пасажира, що отримані відповідними пристроями-зчитувачами на входах до контрольованих зон аеропорту, $\mathbf{R_{інф}}=\{R_{інф1},\dots,R_{інфn}\}$ – потік інформації, що надходить від ресурсів захисту території аеропорту.

Інформаційні потоки для взаємодії системи складають: F_{ikod} – цифровий код (ідентифікатор), отриманий від RFID-мітки *i*-го працівника чи пасажира, $i=\overline{1\dots n}$; $\mathbf{G_v}=\{G_{v1},\dots,G_{vn}\}$ – послідовність оцифрованих кадрів у вигляді зображень у форматі BMP, що надходять від відеокамер; $\mathbf{G}'=\{G_1',\dots,G_n'\}$ – послідовність кадрів для відображення поточної обстановки та місцезнаходження особистості на території аеропорту; $\mathbf{P}=\{P_1,\dots,P_\eta\}$ – виявлені суб'єкти погроз; $\mathbf{W}=\{W_1,\dots,W_\lambda\}$ – множина параметрів, що контролюються та аналізуються для визначення категорії суб'єктів погроз; $S_i^{\text{Fikod}}(x_n,y_n)$ – координати місцезнаходження *i*-ої особи на території аеропорту, $i=\overline{1\dots n}$.

Керуючими впливами виступають: F_{ikodz} – ідентифікатор *i*-ої особи, місцезнаходження якої необхідно визначити; I_{rez} – рішення про ідентифікацію; V_ξ – рішення СППР із виявлення та попередження суб'єктів погроз на території аеропорту.

Вихідним параметром системи є інформативний вектор $\mathbf{W}^*=\{W_i\}$, $i=1\dots\lambda$, який передається каналами зв'язку як електронне повідомлення у відповідні служби безпеки як аеропорту, так і, у разі потреби, до зовнішніх силових структур.

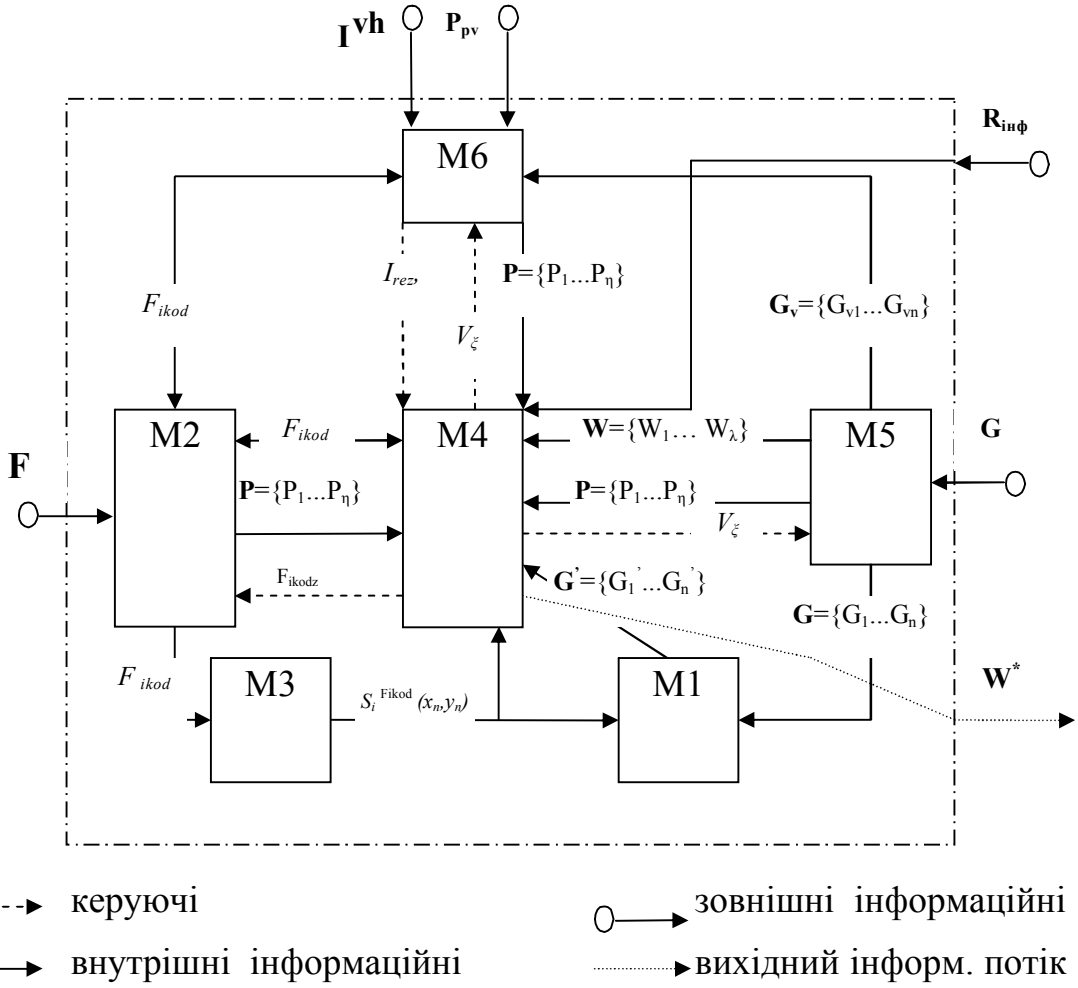

Рис. 2. Модель взаємодії компонентів АСЗ території аеропорту від НСД

Кожен модуль системи є окремою автоматизованою інтегрованою системою. Спроби реалізації несанкціонованого доступу до території аеропорту можливі, як зі сторони персоналу (**N**), так і зі сторони пасажирів (**Z**), хоча можливий і комбінований підхід до реалізації несанкціонованого доступу через потік пасажирів та потік персоналу ($\mathbf{N} \bigcup \mathbf{Z}$). Уся територія аеропорту поділена на певні зони, доступ до яких та системи захисту визначаються в установленому порядку. Ці зони створюють «рубежі» (межі) захисту території аеропорту, які пропонується розглядати як складові концепції побудови АСЗ території аеропорту від НСД.

Отже, отримуємо наступні відкриті класифікаційні угрупування:

$\mathbf{N} = \bigcup_{\gamma} N_{\gamma}$ – множина персоналу, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність авіації;

$\mathbf{Z} = \bigcup_{j} Z_j$ – множина потоку пасажирів, який може бути задіяний у проведенні або підготовці актів незаконного втручання в діяльність авіації.

Таким чином, визначаємо джерела небезпеки у вигляді множини суб'єктів погроз (**P**), які можуть реалізувати спроби несанкціонованого доступу до території аеропорту через потік пасажирів (**Z**) або (та) персонал (**N**), які, в свою чергу, можуть здійснити дії (впливи) VPL^{zn} на об'єкти ураження (**X**) та спровокувати виникнення позаштатної ситуації (ПС):

$$\mathbf{P} = \mathbf{N} \bigcup \mathbf{Z} = (N \setminus Z) \vee (Z \setminus N) \vee (Z \wedge N) \qquad (1)$$

Аналіз функціонування аеропорту виявив потенційні об'єкти ураження, можливість проведення терористичних актів або інших дій на яких матиме максимальний вражаючий

вплив. До таких об'єктів пропонується віднести: повітряні судна (X_1^p); аеровокзальний комплекс (X_2^p); командно-диспетчерський центр управління повітряним рухом (X_3^p); сховища паливно-мастильних матеріалів (ПММ) (склад ПММ, центральні станції заправлення, резервуари котельних установок, цистерни з авіа ПММ, станції перекачування палива) (X_4^p); об'єкти водозабезпечення (резервуари з чистою водою та насосні станції) (X_5^p); авіаційно-технічна база (X_6^p); вантажний термінал (X_7^p); системи електрозабезпечення (X_8^p).

У результаті проведених досліджень сформовано множину позаштатних ситуацій – $\mathbf{Q}$. ПС на об'єкті ураження, визначена на множині суб'єктів погроз та множині ймовірних впливів визначається на множині засобів ураження Q_φ^{pvs} наступним чином:

$$Q_\varphi^{pvs} = \{W_\lambda \mid \lambda = \overline{0,n}\}, \tag{2}$$

де n – кількість засобів ураження.

Інформаційний вектор ПС представлено у вигляді:

$$I_{q_i}^{pvs} = \{W_\lambda, VPL_\iota^{zn}, P_\eta, X_\alpha \mid \lambda = \overline{0,n}, \iota = \overline{0,k}, \eta = \overline{0,(N_\gamma + Z_j)}, \alpha = \overline{0,n_{ou}}\}, \tag{3}$$

де n =10.

Категорія ПС Q_φ^{pvs} визначається як інтегральний показник W_λ, $\lambda = \overline{0,n}$:

$$Q_\varphi^{pvs} = f(W_\lambda) \tag{4}$$

Відповідно до (4) визначається категорія ПС та приймається рішення про залучення відповідних ресурсів для її ліквідації.

Пропонується модель процесу виявлення та ліквідації проявів суб'єктів погроз виникнення ПС у зоні загального доступу території аеропорту (рис. 3). Вона складається з блоку виявлення суб'єктів погроз (БВП) та блоку управління системи (БУС). БВП у своєму складі містить блок спостереження за зоною (В1), блок виявлення суб'єктів погроз виникнення ПС (В2), блок передачі інформації про можливу загрозу виникнення ПС (В3). БУС складається з блоку аналізу вхідної інформації (В4), блоку визначення рівня небезпеки суб'єктів погроз (В5) та блоку прийняття управлінського рішення (В6).

БВП спрямований на спостереження за потоком персоналу (**N**) та потоком пасажирів (**Z**) з метою виявлення суб'єктів погроз (P_η) виникнення ПС на території аеропорту та формування інформаційного вектору ПС $I_{q_i}^{pvs}$. Блок В3 формує інформаційний вектор $I_{q_i}^{pvs}$ та передає його в БУС. Блок (В4) здійснює аналіз вхідної інформації, визначає множину $\mathbf{W}$ та передає інформацію в блок визначення рівня небезпеки суб'єктів погроз (В5), на виході якого ми отримуємо класифікаційний показник даного суб'єкту (суб'єктів) погроз (Q_φ^{pvs}). Залежно від даного показника в блоці В6 формується відповідне управлінське рішення (V_ξ), яке видається оператору служби безпеки аеропорту. Вихідними даними системи є інформаційний вектор $\mathbf{W}^*$, що передається до відповідних силових структур для забезпечення локалізації чи ліквідації негативних впливів суб'єктів погроз із метою попередження виникнення ПС на території аеропорту.

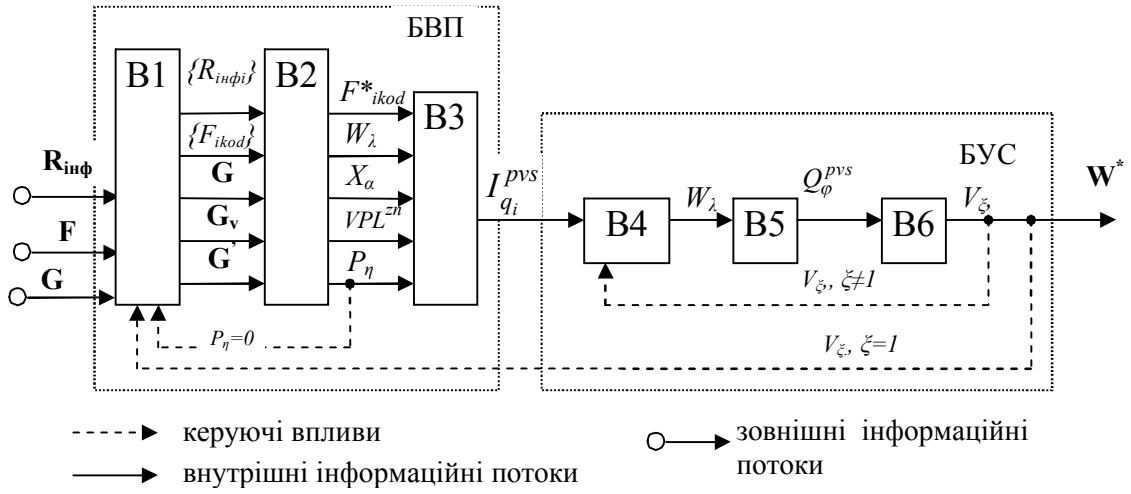

Рис. 2 Модель процесу виявлення суб'єктів погроз у зоні загального доступу території аеропорту

Пропонується модель процесу виявлення суб'єктів погроз у контрольованих зонах аеропорту, які представлено на рис.3 відповідно.

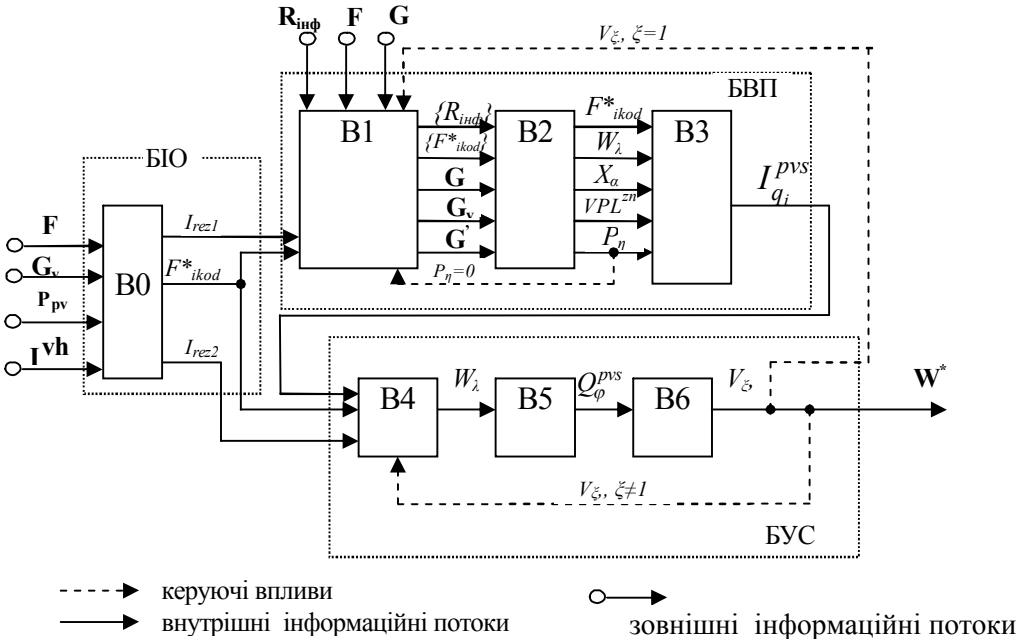

Рис.3. Модель процесу виявлення суб'єктів погроз у контрольованих зонах аеропорту

Модель складається з блоку ідентифікації особи (БІО), в основу якого покладено варіювання біометричних методів ідентифікації, методів розпізнавання образів та інформаційних технологій безконтактної радіочастотної ідентифікації (RFID-технологій); блоку виявлення суб'єктів погроз (БВП); блоку управління системи (БУС).

На вхід блоку ідентифікації особистості (B0) надходять: множина сигналів RFID-міток (**F**), послідовність звукових файлів *i*-го мовця ($\mathbf{I^{vh}}$), послідовність зображень папілярного відбитку *i*-го працівника чи пасажира ($\mathbf{P_{pv}}$), потік відеоданих, що надходить із відеокамер ($\mathbf{G_v}$). У результаті роботи цього блоку отримуємо F^*_{ikod} – цифровий код (ідентифікатор), отриманий від RFID-мітки *i*-го працівника чи пасажира та розпізнаний в підсистемі безконтактної радіочастотної ідентифікації та результуючий вектор (I_{rez}). При позитивному проходженні процедури аутентифікації система приймає рішення I_{rez1} «прохід дозволити» та подає команду на відкриття проходу, при негативному I_{rez2} «заборонити» – блокує прохід та формує повідомлення про загрозу виникнення ПС.

Робота блоків В1 В4, В5, В6 моделі процесу виявлення та попередження ПС у контрольованих зонах аеропорту та В1 В4, В5, В6 моделі виявлення та попередження ПС у зоні загального доступу території аеропорту ідентичні.

Відмінністю є те, що блок В2 БВП у контрольованих зонах аеропорту працює у режимі спостереження за зоною з метою виявлення суб'єктів погроз P_η шляхом визначення показника девіантної поведінки W_1 пасажирів та персоналу. При виявленні таких суб'єктів, система, керована оператором, проводить ідентифікацію даного суб'єкту (F^*_{ikod}) погроз та визначає показники $W_2 \div W_{10}$, X_α, VPL^{zn}. Після цього В3 формує інформаційний вектор $I_{q_i}^{pvs}$ та передає його в БУС для аналізу W_λ (В4), визначення рівня небезпеки Q_φ^{pvs} (В5), прийняття управлінського рішення V_ξ (В6).

Запропоновані моделі дозволяють автоматизувати процес прийняття управлінських рішень оператором служби безпеки аеропорту щодо виявлення суб'єктів погроз виникнення ПС та сповіщення відповідних ресурсів захисту для ліквідації їх проявів.

Висновки. В результаті проведених досліджень запропоновано структуру АЗС території аеропорту від НСД, побудовано модель взаємодії компонентів системи, процесу виявлення суб'єктів погроз у зоні загального доступу та контрольованих зонах аеропорту. Сформовано множину суб'єктів погроз та визначено інформаційний вектор позаштатної ситуації на території аеропорту.

Список літератури

1. *Пюшки Л.* Методы и средства построения автоматизированных интегрированных систем защиты особо важных объектов: дис…канд.техн.наук: 05.13.06 / Пюшки Ласло.– К., 2005.– 156 с.
2. Інтелектуальні системи: навч.посібник /*[Ю.О. Колос, А.І. Бобунов, О.М. Перегуда та ін.]; під ред. Б.М. Герасимова*.– Житомир:ЖВІ НАУ,2008.–176 с.
3. *Герасимов Б.М.* Системы поддержки принятия решений: проектирование, применение, оценка эффективности: Монографія / Б.М. Герасимов, М.М. Диви-зинюк, И.Ю. Субач. – Севастополь: Гос. Океанариум, 2004. – 320 с.
4. *Биченок М.М.* Основи інформатизації управління регіональною безпекою. – К.Інститут національної безпеки, 2005. – 196 с.
5. *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.
6. *Палагин А.В.* Системная интеграция средств компьютерной техники: монография / А.В. Палагин, Ю.С.Яковлев – Винница: «УНІВЕРСУМ–Вінниця», 2005. – 680 с.
7. *Васюхин М.И.* Алгоритмические и программно-аппаратные методы и средства построения интерактивных геоинформационных комплексов оперативного взаимодействия: дис. … докт. техн. наук: 05.13.13 / Васюхин Михаил Иванович. – К., 2002. – 414 с.

Рецензент: Дудикевич В.Б.
Надійшла 28.09.2010