3. *Гурєєв В.О.* Розробка алгоритмів і програм швидкодіючих методів розрахунку режимів роботи великих електроенергетичних систем (ЕЕС) і енергооб'єднань (ЕО) для тренажерів // Наукові праці ВНТУ, – 2018, № 1, С.1-5.
4. *Гурєєв В.О.* Моделювання великих енергосистем для побудови комп'ютерних розподілених тренажерних систем в енергетиці // Моделювання та інформаційні техноло-гії. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Вип. 83. – К.:2018. – С.94-105.
5. *Гуреев В.А.* Построение обучающего дистанционного тренажера для подготовки персонала энергетической отрасли / В. А. Гуреев, О. В. Сангинова. // Праці Інституту електродинаміки НАНУ. – 2017. – С.52-58.
6. *Гуреев В.А.* Принципы организации национальной системы обучения и тренажа персонала объединенной электроэнергетической системы Украины / В. А. Гуреев, В. Д. Самойлов, О. В. Сангинова. // Электронное моделирование. – 2016. – №4. – С. 109–121.
7. *Воропай Н.И.* Упрощение математических моделей динамики электроэнергетических систем, Новосибирск: Наука, Сиб. отделение, 1981.
8. *Ананичева С.С., Музин А.Л.* Схемы замещения и установившиеся режимы электрических сетей: Учеб. пособие, Екатеринбург: УрФУ, 2011.

http://doi.org/10.5281/zenodo.3612250

Поступила 12.09.2019р.

УДК 004.02+004.05+005.93+ 510.3

Є.С. Родін, Київ

ОСОБЛИВОСТІ ПОБУДОВИ МОДЕЛЕЙ БЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Abstract. The architectural principles of the of distributed information systems operation are disclosed. A projection of the information security system was built taking into account the architectural characteristics of distributed information systems. The interconnections of security system elements with elements of distributed systems are determined. The principles of modeling security systems for distributed systems are proposed.

Вступ. Швидкий розвиток інформаційних технологій пропонує нові підходи до автоматизації в таких напрямках діяльності, як розв’язання наукових задач, підтримка процесів прийняття рішень, обробка безперервних транзакцій даних, інформаційне обслуговування бізнес-процесів та ін. Практично жодне з перелічених завдань сьогодні не вирішується локально. Можливість доступу до відносно дешевих розподілених інформаційно-обчислювальних потужностей переважає ризики виведення цінної інформації в слабозахищені масоводоступні розподілені інформаційні системи. Актуальним завданням наразі стає адаптація або створення нових підходів і методів щодо захисту інформації тепер уже в динамічних системах розподіленої в просторі та

часі архітектури.

Задачею автора є розробка вимог щодо моделювання та функціонування системи безпеки для розподіленої інформаційної системи. У рамках цієї задачі пропонуються визначення для елементів системи безпеки, її головні характеристики функціонування, міри ефективності функціонування системи безпеки.

Традиційний підхід до вирішення задач захисту інформаційних систем полягає в забезпеченні необхідного рівня безпеки всіх компонент системи і, в тому числі, розподілених інформаційних систем (*RIS*) в цілому. Оскільки *RIS* розподілена не тільки функціонально, але і просторово, з погляду територіального розміщення її компонент, то розв'язання задачі захисту системи *RIS* є досить складним [1]. У багатьох випадках необхідний рівень безпеки *RIS*, в цілому, не може бути забезпечений. Це обумовлено тим, що по відношенню до різних компонент системи в її зовнішньому інформаційному та функціональному середовищі завжди будуть існувати небезпеки, характер яких може бути штучним і упередженим, або природним і випадковим, і вони можуть постійно активізувати загрози для *RIS*. Тому виникає задача локального, в часі і просторі, убезпечення окремих компонент *RIS*. Локальним рівнем безпеки в часі будемо вважати інтервал часу, протягом якого гарантується необхідний рівень безпеки. Локальним рівнем безпеки в просторі будемо вважати рівень безпеки окремої компоненти всієї системи, який будемо також називати рівнем безпеки окремого ресурсу системи *RIS*. Введемо визначення термінів, що стосуються безпеки *RIS*, якими будемо користуватися в рамках статті та які не протирічать інтерпретації відповідних загальноприйнятих термінів.

Визначення 1. Небезпекою (*Nb*) будемо називати фрагмент зовнішнього середовища *RIS*, який може формувати загрозу по відношенню до окремих компонент системи.

Визначення 2. Загрозою (*Zg*) будемо називати процес або об'єкт, який формується *Nb* таким чином, щоб останній, в рамках своїх внутрішніх можливостей, міг активізувати атаку на компоненти *RIS*.

Визначення 3. Атакою (*At*) будемо називати процес, який активізується відповідною загрозою в середовищі атакованого об'єкта.

Таким чином, процес негативної взаємодії оточуючого середовища з компонентами *RIS* можна відобразити такою схемою: $Nb \rightarrow Zg \rightarrow At$. Слід відмітити, що зовнішнє середовище для *RIS* являє собою не тільки фізичне середовище, в якому розподілені компоненти *RIS*, а й інформаційне середовище, тобто середовище користувачів та інші типи середовищ, де можуть виникати *Nb*, які будуть формувати *Zg*, а останні можуть активізувати *At* для реалізації впливу на довільну компоненту системи і на *RIS* в цілому.

Розподілені системи характеризуються розподіленістю в просторі, часі, розподіленістю по типу ресурсів, функціональною розподіленістю та розподіленістю по відношенню до користувачів. Тому доцільно систему

безпеки (*SB*), яка реалізує процеси захисту в *RIS*, будувати таким чином, щоб вона була розподілена не тільки просторово, що обумовлюється просторовою розподіленістю компонент *RIS*, а також розподілена між ресурсами в часі, могла розподілятися на основі функціональних характеристик окремих ресурсів. Опис основних характеристик *SB* передбачає наявність таких ознак:

- керованість;
- міра захисту та величина безпеки, яка може бути пов'язана з мірою захисту;
- оцінка величини ризику, яка, на відміну від величини безпеки, характеризує розміри втрат, що виникають по відношенню до об'єкта предметної області;
- здатність реалізовувати динамічні процеси захисту;
- здатність адаптуватися до необхідної міри захисту, який реалізується системою SB по відношенню до кожної окремої компоненти.

Керованість у даному випадку означає, що учасник процесу функціонування *RIS* (як правило, ним є системний адміністратор) під час експлуатації *RIS* може міняти засоби захисту, що знаходяться в *SB*, для окремих компонент системи *RIS*. Така інтерпретація керованості *SB* є зрозумілою і реалізується в усіх типах інформаційних систем, якщо система потребує реалізації керованості. Важливою особливістю керованості по відношенню до прикладних процесів є те, що вона не здійснюється в періоди їх функціонування. Можна стверджувати, що керування в цьому випадку здійснюється в процесі налагодження системи на виконання тої чи іншої прикладної задачі.

Поняття про міру захисту та величину безпеки досить часто використовують як такі, що мають у галузі захисту інформації рівнозначні інтерпретації. В рамках даної статті ці два терміни будемо інтерпретувати дещо по-різному. Міру захисту будемо відносити до системи безпеки, яка таку міру може визначати, оскільки сам термін передбачає введення деякої шкали вимірювань. Прикладом такої міри може бути кількість раніше не відомих атак, відбитих системою *SB* за певний період функціонування *RIS* або протягом функціонування певної кількості прикладних задач у *RIS*. Таке визначення є прийнятним, оскільки по відношенню до відомих атак використовуються відомі засоби захисту, які, за визначенням, повинні успішно протидіяти відповідним атакам.

Величина безпеки відображає результати захисту об'єктів або процесів, що мають місце в *RIS*. Це означає, що загрозі не вдалося здійснити негативний вплив на об'єкт захисту шляхом активізації атаки. Цей результат вимірюється кількістю втручань загрози за допомогою атак у процес розв'язування прикладної задачі за встановлений певним чином період функціонування цієї задачі в *RIS*. У запропонованій інтерпретації міра захисту залежить від кількості різних та нових атак, які були відбиті системою *SB*, а величина безпеки залежить від кількості відомих або передбачуваних атак, включаючи атаки, які повторювалися.

Поняття ризику відноситься до об'єкта, що захищається системою *SB*, і, як відомо, відображає величину втрат, яких зазнає об'єкт атаки в результаті її успішного завершення. Помилковим є співставлення поняття ризику з рівнем безпеки атакованого об'єкта, хоча би через те, що величина ризику (*r*) може дорівнювати нулю тільки завдяки тому, що небезпека не ініціювала загрозу, а загроза не активізувала атаку під час функціонування прикладної задачі. Якщо система *SB* успішно виконала свої задачі захисту, а це означає, що величина безпеки не дорівнює нулю, і небезпека не ініціювала нових загроз, то незважаючи на те, що небезпека виявляла активність по відношенню до об'єкта захисту, ризик залишається рівним нулю. Тому величину ризику слід розглядати як умову, на основі якої формуються вимоги до величини безпеки та міри захищеності, що їх повинна забезпечувати система *SB*.

Переважно, система *SB* розглядається як система, що ідентифікує відомі загрози й атаки, розпізнає нові загрози й атаки, протидіє тією чи іншою мірою відповідним атакам та пов'язана певним чином з компонентами, які вона захищає [2]. Для ефективнішого використання *SB* в *RIS* доцільно мати можливість, залежно від поточної потреби, використовувати одні й ті самі засоби *SB* для різних компонент. У цьому випадку особливого значення набуває можливість організації динамічного процесу використання засобів *SB* в *RIS*. Засоби захисту (*Zz*), які входять до складу *SB*, можуть являти собою окремі системи моніторингу втручань *IDS*, що безпосередньо зв'язані з різними компонентами *RIS* і з елементами, котрі реалізують задачі розпізнавання та ідентифікації атак. У рамках архітектури загальної системи моніторингу втручання *CIDF* (*Common Intrusion Framework*) існує можливість організації окремих компонент таким чином, щоб фрагменти захисту можна було використовувати спільно для більшості компонент *RIS*. У цьому випадку можна говорити про динамічне використання елементів типу *IDS*. Для забезпечення здатності адаптуватися до заданої міри захисту, що реалізує *SB*, необхідно повніше враховувати організацію функціонування системи типу *CIDF* та додаткові вимоги до прикладних систем і прикладних задач, які розв'язуються в цих системах [3].

Хмарні технології, засобами реалізації яких є системи типу *RIS*, на відміну від *RIS*, називаються прикладними системами [4]. Значна кількість задач прикладних систем потребує захисту процесів їх розв'язання з різних причин, наприклад, через необхідність зберігати таємниці, через вартість інформації або через їх класифікацію та ін. Тому забезпечення необхідного рівня безпеки процесів розв'язання таких задач у рамках *RIS* є актуальним. В цілому захищати систему типу *RIS* в більшості випадків досить складно. Для вирішення цієї проблеми потрібні нові підходи, які б дозволили тією чи іншою мірою забезпечувати можливість захисту прикладних задач. Основні елементи цього підходу стосовно систем *RIS* потребують реалізації таких завдань:

- система захисту об'єктів типу RIS має бути розподіленою системою безпеки (RSB), що обслуговує RIS , але функціонує як незалежна від

RIS система; в певному наближенні можна говорити про синтез двох систем − RIS і RSB, які розв'язують прикладну задачу, де RIS забезпечує реалізацію розв'язання прикладної задачі, а RSB − безпеку процесу розв'язання;

- система RSB повинна забезпечувати можливість управління динамічними процесами, пов'язаними з убезпеченням компонент, що використовуються для розв'язання прикладної задачі, якими є, в першу чергу, компоненти прикладної системи задач та RIS;
- система RSB повинна включати засоби управління процесами адаптації RSB до вимог щодо захисту інформації та процесів розв'язання прикладної задачі, які задаються в початкових умовах у вигляді вхідних даних і вимог, що можуть виникати в процесі розв'язання прикладних задач.

Перш ніж формулювати вимоги до прикладної системи типу *RIS*, розглянемо її основні структурні особливості. Прикладами прикладних систем розв'язання задач користувача (*PSZ*) можуть слугувати система управління логістикою транспортної фірми, система бухгалтерського управління та інші. Ілюстрацією прикладних задач, що розв'язуються в рамках відповідних прикладних систем в першому прикладі, можуть бути задачі визначення оптимального трафіка виконання замовлення з транспортування вантажу або задача планування замовлень на регулярні перевезення та інші. Ілюстрацією прикладних задач, що розв'язуються в другому прикладі прикладної системи, є задачі нарахування місячної заробітної плати працівникам фірми, задача складання фінансового звіту за вибраний період часу та інші. В задачі складання фінансового звіту можуть бути виділені окремі компоненти, які є прикладними задачами наступного рівня, такі, наприклад, як формування розділу звіту по затратах на матеріальні ресурси і розділу звіту по затратах на виконання окремих замовлень щодо обслуговування та інші. Розподіл задач окремого рівня, який визначає їх близькість до прикладної системи, може бути продовжений, якщо це дозволяє інтерпретація предметної області досліджуваної задачі. З наведених прикладів видно, що створення структури окремої прикладної задачі базується на аналізі інтерпретації відповідних підзадач.

У рамках прикладної системи *PSZ*, в якій передбачається розв'язувати певні задачі користувача, мають бути виконані такі вимоги:

- систему PSZ необхідно представити у вигляді системи, яка є результатом синтезу двох структур, одна із цих структур відображає рівень захисту для кожної задачі, а інша – сукупність елементів, кожний з яких є окремою прикладною задачею;
- у кожному елементі структури прикладної задачі мають бути вказані типи та способи його реалізації (елемент, що являє собою програмну реалізацію окремого алгоритму; елемент, що є окремим фрагментом числових даних; елемент, що є інтерпретаційним описом деякого іншого елемента, наприклад, окремого фрагмента даних, і т.п.);

– система PSZ має бути розподіленою прикладною системою (RPS) та повинна організовувати таку взаємодію з системою RSB, яка забезпечує передачу системі RSB даних про необхідні рівні захисту та засоби інтерпретації відповідних рівнів захисту.

У зв'язку з наведеним вище підходом до організації розподіленого процесу захисту прикладної системи, що реалізується в рамках *RIS* та відповідними прикладними задачами, виникає необхідність розв'язати такі задачі:

1. Побудувати модель безпеки, яка реалізує вибір стратегії надання ресурсів для захисту RPS таким чином, щоб забезпечити необхідний рівень безпеки для кожної прикладної задачі, а також окремого ресурсу, використовуваного у відповідній задачі, якщо в цьому виникає потреба.
2. Дослідити міру впливу величини рівня безпеки окремої прикладної задачі (Zai) на загальну величину безпеки прикладної системи.
3. Дослідити міру взаємного впливу рівнів безпеки між парами вибраних захищених ресурсів, що виділені в RPS, для захисту відповідних прикладних задач, якщо останні взаємодіють між собою.

Визначимо початкові умови, необхідні для розв'язання задачі побудови моделі захисту. Система захисту описує способи реалізації процесів захисту, тому будемо говорити про модель *M*(*SB*). Оскільки *SB* є розподілена, то і модель буде враховувати таку розподіленість, що будемо позначати *M*(*RSB*). Вхідною інформацією для функціонування такої моделі будуть дані про атаки At_i, що активізовані відповідними загрозами Zg_i. У випадку існування деякої Zg_i або коли Zg_i сформована відповідною Nb_i, загроза визначає випадковим способом значення моменту активізації відповідної At_i та значення параметрів, що обумовлюють її різновид випадковим для об'єкта атаки чином.

Розглянемо детальніше задачі, які мають розв'язуватися в *M*(*RSB*):

1. Виявлення і розпізнавання Ati, що орієнтована на окремий об'єкт атаки;
2. Виявлення аномалії в потенційних небезпеках, що може призводити до виникнення Zgi і, відповідно, Ati;
3. У разі виявлення аномалії в Zgi засоби M(RSB) повинні реалізовувати превентивні заходи, які заблокують можливість Zgi активізувати атаку.
4. Визначення класу елементів системи RPS, для яких тип виявленої атаки може бути небезпечним, окрім елемента, на який атака скерована;
5. Розпізнавання та оцінювання загрози, яка визначається моделлю для RPS;
6. Реалізація протидії новій виявленій Ati засобами M(RSB) та визначення ризику для фрагмента RPS, що містить у собі атакований елемент.

7. Оцінювання засобами M(RSB) загальної величини безпеки для функціонування RPS на даний момент.

Будь-які атаки, що реалізуються на компоненти *RPS*, використовують наявні в системі канали, через які до відповідних компонент у процесі розв'язання прикладних задач передається інформація − дані, інформація для керування процесом розв'язування задач, інші види інформації, що передбачені системою організації роботи *RIS*. Згідно з визначенням (3), атака являє собою процес, що активізований у середовищі об'єкта атаки. Це означає, що виявлення довільної атаки має базуватися на аналізі відповідності даного фрагмента та відповідності процесів, що реалізуються в ньому, всім параметрам, які характеризують функціонування об'єкта в штатному режимі. Оскільки в компонентах *RIS* постійно реалізуються різні процеси, то параметри, що їх характеризують, постійно змінюються. Тому привести процес розпізнавання атак до класичних методів розпізнавання образів складно. Це зумовлює необхідність розділити процес виявлення атак на такі частини:

- виявлення недопустимих відхилень або аномалій у процесах, що відбуваються у фрагменті, в якому реалізується штатний режим розв'язання прикладної задачі;
- на основі виявлених параметрів аномалій, використовуючи еталони існуючих атак, сформувати опис еталону виявленої атаки і ним розширити перелік існуючих еталонів атак;
- розпізнавання за виявленою аномалією атаки таким чином, щоб на основі даних, отриманих у результаті розпізнавання, можна було формувати подальші дії, пов'язані з реагуванням на виявлену атаку.

Оскільки аномалія, за своєю суттю, є об'єктом достатньо невизначеним, то у відомих методах її виявлення задіяні способи, для яких характерним є використання засобів, що оперують приблизними даними [5]. Класичний приклад − статистичні методи, які для аналізу замість точних даних використовують множини даних про досліджуваний об'єкт. Відповідно до зазначеного, виникає задача вибору необхідного способу виявлення та опису аномалій і, як наслідок, атак. Коли планується використовувати статистичні методи, то основними ознаками аномалій є статистичні параметри (наприклад, значення таких характеристик, як математичне очікування, дисперсія, статистичні моменти різних порядків та ін.). Цей підхід буде найбільш ефективним для випадків, коли аномалія є невідомою для засобів виявлення. Способи виявлення аномалій досить широко досліджуються, а розробка засобів їх реалізації надає широкий вибір пристроїв, відомих як *IDS*.

Класичним прикладом системи розпізнавання атак для випадку, коли інформація про атаки відома, є використання експертних систем, які формуються на основі даних, що надаються експертами в галузі захисту інформаційних систем про ті чи інші атаки [6]. Оскільки атаки являють собою процеси, то образ таких атак формується у вигляді правил, що описують послідовність реалізації цих процесів. Сукупність таких правил

становить основну частину експертної системи виявлення атак. На практиці, більшість атак активізується під контролем і з участю фахівців, які є проєктантами відповідних загроз і атак. Тому в чергових атаках способи їх реалізації можуть модифікуватися. Це призводить до зниження рівня безпеки, який повинна забезпечувати система *RSB*. Задля усунення цього недоліку при побудові системи *RSB* використовують підходи, що базуються на принципах, які здатні реалізовувати розпізнавання певних відхилень в описах атак по відношенню до їх еталонних описів. Завдяки цьому відповідні системи здатні ідентифікувати тип атаки з певними мірами їх наближень, якщо вони мають деяку модифікацію [7]. У цьому випадку виникає необхідність відтворювати відповідні модифікації та формувати в експертній системі еталонні описи модифікованих атак. Прикладом систем, які розпізнають атаки, подібні до відомих атак, але є модифікованими атаками, можуть бути системи безпеки, побудовані на основі використання нейронних мереж. Відомо, що нейронні мережі в результаті реалізації в них процедур навчання, яке являє собою настроювання мережі на розпізнавання образів певних типів атак, спроможні розпізнавати не тільки атаки, що мають точний опис, а й атаки, які певною мірою відрізняються від описів атак, що використовувалися в процесі навчання. Система безпеки, побудована на використанні нейронних систем, не тільки розпізнає модифіковані атаки, а й визначає міру відхилення модифікованої атаки від атаки, що описується еталоном.

Щоб виявляти, розпізнавати та протидіяти атакам, системам *RSB* потрібні такі можливості:

1. Здійснювати оперативну протидію Ati, оскільки процес впливу Ati на RPS може розпочинатися ще під час активізації Ati.
2. Розширювати можливості системи RSB стосовно захисту прикладних задач, які передбачається розв’язувати в рамках системи RPS.
3. Встановлювати атаки, які можуть повторюватися в процесі функціонування системи RPS.
4. Виявляти причини виникнення атак і мотивацію їх активізації, яка, в першу чергу, може бути притаманна штучним об’єктам, створеним відповідними фахівцями, а у випадку природних небезпек доцільно виявляти природні закономірності, що обумовлюють виникнення таких небезпек.
5. Виявляти взаємозв’язок, або взаємозалежності між характером прикладних задач і можливими причинами виникнення небезпек, загроз і атак як цілі існування відповідної небезпеки.

Оперативна протидія атаці є природною реакцією на її виявлення, а забезпечення ефекту повної нейтралізації дії атаки на атакований об’єкт стає можливим у таких випадках:

- якщо атака являє собою процес, який можна розділити на окремі етапи відповідно до її взаємодії з середовищем об’єкта атаки;
- якщо існує можливість оперативно встановити ціль реалізації атаки на основі її ідентифікації, або на основі аналізу характеру процесу

реалізації атаки, або відповідно до інших можливих даних про атаку, які не обов'язково можуть проявлятися в процесі її реалізації;

- якщо атака впливає на об'єкт починаючи з моменту її активізації і існує можливість оцінити такий вплив на об'єкт атаки на кожній стадії її функціонування.

Якщо атаку неможливо описати як послідовність реалізації процесу її взаємодії з об'єктом, то це означає, що значення параметрів атаки не сумісні зі значеннями параметрів, що характеризують об'єкт атаки. Наприклад, якщо атака успішно діє на об'єкт протягом інтервалу часу Δt_i , який є менший або рівний встановленому інтервалу часу δt_i, що визначає період реалізації одного кроку функціонування об'єкта атаки, то має місце несумісність параметрів атаки з параметрами атакованого об'єкта.

Протидія атаці може реалізовуватися засобами *RSB* декількома способами:

- якщо відомо, як розпізнаній атаці протидіяти, і алгоритми протидії реалізовані в RSB;
- якщо в RSB не існує відомого алгоритму протидії атаці і необхідно оперативно сформувати такий алгоритм (у більшості випадків це зводиться до відомих модифікацій відповідних алгоритмів);
- якщо атаку виявлено як неідентифіковану або ідентифіковану, але неможливо оперативно сформувати засоби протидії, то блокується фрагмент середовища, в якому виникла атака.

Результатами пошуку принципів побудови розподіленої системи безпеки є: формування бази знань про процеси *RSB*, визначення задач, які має вирішувати система *RSB*, правила моделювання *RSB*.

Висновки. Розуміння масштабу та глибини архітектури сучасних *RIS* зумовлює пошук нових підходів до моделювання керування інформаційною безпекою, де основою є аудит інформаційної системи, визначення інформаційних ресурсів, вразливостей, загроз, оцінювання ризику та розробка заходів щодо його зменшення [8]. Сучасні принципи побудови інформаційних систем на базі мікросервісів також вимагають адекватних швидких та розподілених систем захисту окремих процесів з можливістю масштабування або деактивації процесу.

1. *Радченко Г.И.* Распределенные вычислительные системы: учебное пособие. – Челябинск: Фотохудожник, 2012. – 184 с.

2. *Емельянова Ю.Г., Фраленко В.П.* Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения. – 2011. – № 4(8). – С. 17–31.

3. CIDF Working Group. The common intrusion detection framework. Vesion 0.6, доступне під адресою http://seclab.cs.ucdavis.edu/cidf, 1999.

4. *Rasool Jalili, Fatemeh Imani-Mehr, Mortez a Amini, Hamid Reza Shahriari*. Detection of Distribute Denial of Service Attacks Using Statistical Pre-Processor and Unsupervised Neural Networks // Lecture Notes in Computer Science. – 2005. – Vol. 3439. – P. 192–203.

5. *Upton David M., Creese Sadie.* The Danger from Within // Harvard Business Review. – 2014, September. – №1. – 9 p.
6. *Бигелоу С.* Сети: поиск неисправностей, поддержка и восстановление. – СПб: БХВ-Петербург, 2005. – 1200 с.
7. *Родін Є.С.* Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки // Математичні машини і системи. − 2012. – № 4. − С. 142−148.
8. *International standard* BS ISO/IEC 27005:2008, 2008-06-15.

http://doi.org/10.5281/zenodo.3612252

Поступила 2.09.2019р.

УДК 009.4

Б.М. Гавриш [1], Львів
Б.В. Дурняк [1], Львів
О.В. Тимченко [1, 2], Olsztyn, Poland

АНАЛІЗ МЕТОДІВ ОПРАЦЮВАННЯ СИГНАЛІВ, ЯК ФУНКЦІЙ ПАРАМЕТРІВ ОБ'ЄКТІВ В ІНФОРМАЦІЙНИХ КАНАЛАХ КОМП'ЮТЕРНИХ СИСТЕМ

Abstract. The implementation of modern digital components of computer systems in the field of control, measurement, identification and diagnosis is based on the use of information-measuring channels, which provide the conversion of analog non-electronic quantities into the corresponding electrical ones: amplitude, frequency, phase, etc., with their subsequent processing. The separation of the informative part of the signal from the data stream is traditionally implemented on the statistical methods basis, spectral, correlation and cluster analysis by the mentioned characteristics or their combinations. Correlation is considered to be the most effective of the known ones, however, this approach requires the provision of special forms of signals, since the correlation properties of the latter are crucial in the processing and interpretation For signals that do not have acceptable correlation characteristics, it is advisable to use frequency-time signaling.

Keywords: information system, images, frequency functions

Вступ

Існуючі на сьогодні задачі та проблеми автоматичного аналізу зображень вимагають створення ефективних методів їх високорівневого опрацювання та аналізу. Аналізуючи практично розроблені на сьогодні підходи, які вирішують згадані задачі, можна зробити висновок, що практично для кожного окремого класу задач та зображень існує окремий набір засобів для їх вирішення шляхом

[1], Українська академія друкарства
[2] University of Warmia and Mazury in Olsztyn