УДК 681.3.06

ВЛАСТИВОСТІ ДІЯЛЬНОСТІ ІЗ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ЯК СИСТЕМНОЇ КАТЕГОРІЇ

О.В. ПОТІЙ, Д.Ю. ПИЛИПЕНКО, Д.І. ГЛАДКИЙ

В роботі досліджуються властивості діяльнісного аспекту захисту інформації як системної категорії. Сформована множина властивостей дозволяє різнобічно оцінювати діяльність із захисту інформації. Наведена множина властивостей також становить певну основу для подальшого дослідження та розробки аналітичних виразів та критеріїв оцінки організаційної системи захисту інформації.

Ключові слова: системодіяльнісний підхід, діяльність із захисту інформації, оцінювання.

ВСТУП

У більшості випадків захист інформації як об'єкт досліджень не враховує аспект людської діяльності, або ж йому приділяється не достатньо велика увага. Проте, діяльнісний аспект відіграє значну роль в інформаційній безпеці, і сьогодні можна із впевненістю казати, що серед фахівців формується певний інтерес до розглядання проблем інформаційної безпеки у рамках системодіяльнісного підходу.

Розглядаючи захист інформації як діяльність, слід зазначити, що ця системна категорія характеризується певними властивостями та характеристиками. Властивості – це об'єктивні особливості діяльності, які проявляються під час її здійснення. Захист інформації в свою чергу може бути охарактеризований з точки зору ефективності, цілеспрямованості, безперервності, організованості, керованості, узгодженості тощо. Виявлення, розкриття змісту, систематизація та опис цих та інших властивостей діяльності, визначення показників та критеріїв їх оцінювання, формування відповідних теоретичних, науково-методичних основ та розробка інструментарію оцінювання властивостей та характеристик є окремою важливою та актуальною дослідницькою задачею.

1. ОНТОЛОГІЯ ВЛАСТИВОСТЕЙ ЗАХИСТУ ІНФОРМЦАЇ

Як зазначено на рис.1, діяльнісний аспект захисту інформації здійснюється у рамках організаційної системи захисту інформації. Діяльність має певні властивості, а саме: ефективність, зрілість, адекватність, прийнятність, гнучкість, здійсненність та простоту в адміністративному забезпеченні. Ефективність є досить широкою властивістю, що дозволяє досліджувати її на більш глибокому рівні. Ефективність захисту інформації можна розглядати з точки зору результативності, економічності та оперативності.

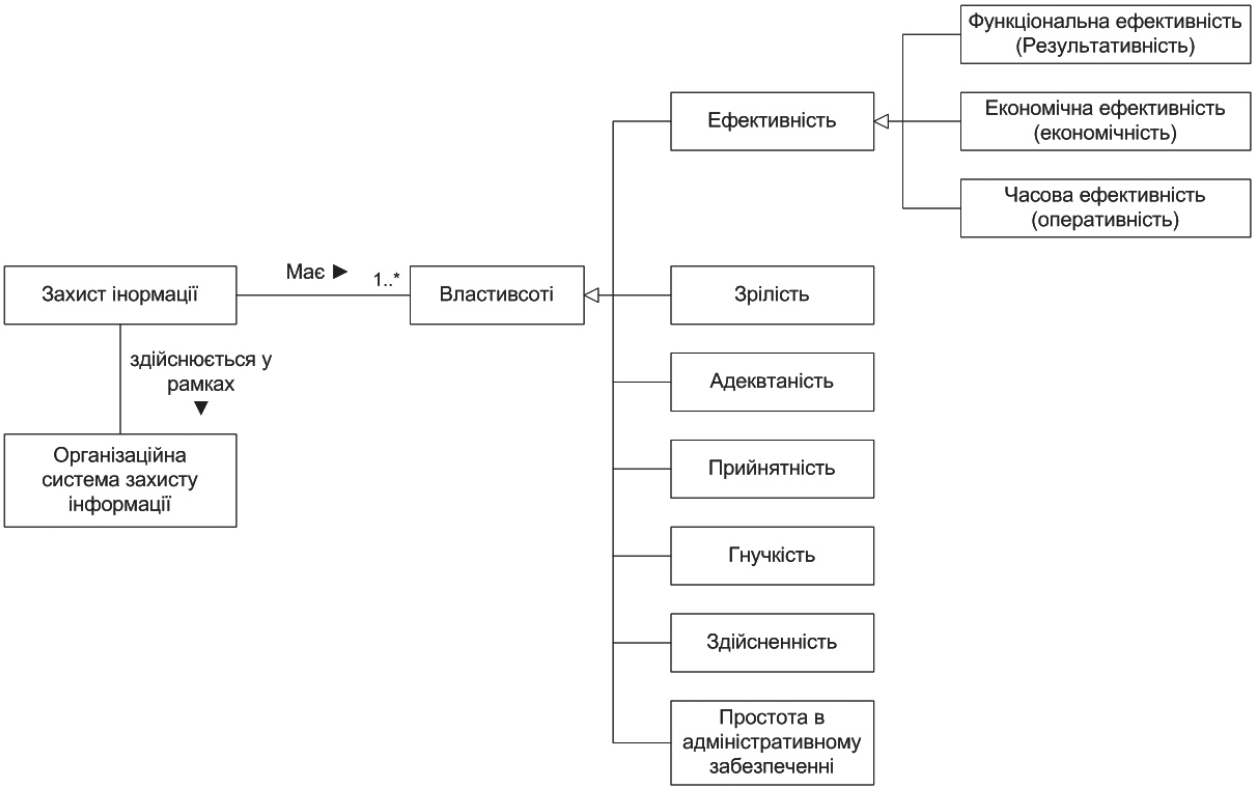

Рис. 1. Проблемно-орієнтовна онтологія властивостей захисту інформації як діяльності

2. ЕФЕКТИВНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ

Одним з найважливіших питань у рамках системодіяльнісної методології є визначення поняття та змісту ефективності захисту інформації. Підвищення ефективності захисту інформації саме як діяльності, тобто у рамках організаційної системи захисту інформації, підвищення ефективності організаційних форм та методів захисту інформації є актуальною задачею як у практиці, так і у теорії захисту інформації. У визначенні ефективності захисту інформації, як діяльності виходитимемо з таких поглядів.

Будь-яка діяльність здійснюється у рамках деякої організаційної системи S_0. По відношенню до цієї системи мета діяльності X_0 є основним системоутворюючим чинником як спосіб інтеграції різних видів діяльності (процесів, дій) у єдину систему. Мета є ідеальним уявленням у свідомості суб'єкта діяльності бажаного результату. Вона визначає способи та форми організації діяльності, характер та системну впорядкованість, а також засоби досягнення мети суб'єктом [1].

Взагалі будь-яка мета у формалізованому вигляді може бути виражена деяким набором бажаних параметрів Y_{mp}. Реальний результат Y діяльності у загальному випадку може не співпасти з тим, що вимагається. У відповідності до усталених поглядів, під ефективністю розуміють співвідношення бажаного результату Y_{mp} до реально досягнутого результату Y. Результат діяльності Y ставлять у залежність від трьох основних результуючі факторів – корисного ефекту Q, затраченого ресурсу C та часу T. Ці фактори залежать від конкретної обраної стратегії u, тобто [1]:

$$Y(u) = Y\big(Q(u), C(u), T(u)\big).$$

Головною метою захисту інформації є досягнення певного рівня захищеності інформації або безпеки інформації. Тому результатом діяльності із захисту інформації, корисним ефектом є певний досягнутий рівень безпеки інформації L_{SI}. На досягнення певного рівня безпеки інформації, суб'єкт захисту витрачає матеріальні, фінансові, людські та інші ресурси C та час T. Рівень безпеки, витрати ресурсів та часу безпосередньо залежать від конкретної обраної суб'єктом захисту стратегії захисту U_{SP}. Таким чином, результат захисту інформації може бути поданий як

$$Y(U_{SP}) = Y(L_{SI}(U_{SP}), C(U_{SP}), T(U_{SP})).$$

Під ефективністю захисту інформації розумітимемо співвідношення бажаного результату захисту інформації (у термінах рівня безпеки інформації, витрат ресурсів та часу) та реально досягнутого результату.

Спираючись на підходи щодо класифікації ефективності у різних сферах діяльності [1, 2, 3, 4] у подальшому пропонується розрізнювати функціональну ефективність, економічну ефективність та часову ефективність захисту інформації.

Функціональна ефективність або *результативність* захисту інформації є ступінь відповідності реального рівня безпеки інформації L_{SI} тому, що очікувався або вимагався L^*_{SI}, тобто

$$Э_f(U_{SP}) = f(L_{SI}(U_{SP}), L^*_{SI}).$$

Під *економічною ефективністю* або *економічністю* захисту інформації розумітимемо співвідношення досягнутого рівня безпеки інформації L_{SI} та затраченого ресурсу C, тобто

$$Э_\rho(U_{SP}) = \rho(L_{SI}(U_{SP}), C(U_{SP})).$$

Під *часовою ефективністю* або *оперативністю* розумітимемо співвідношення досягнутого рівня безпеки інформації L_{SI} до часових витрат T, що понесені на досягнення цього рівня, тобто

$$Э_\tau(U_{SP}) = \tau(L_{SI}(U_{SP}), T(U_{SP})).$$

Таким чином, ефективність захисту інформації є узагальнена визначальна функціональна властивість системи захисту інформації, у рамках якої здійснюється ця діяльність, яка з гносеологічної точки зору розкривається через категорію мети (тобто рівня безпеки) та об'єктивно виражається ступенем досягнення мети захисту інформації X_0 з урахуванням витрат ресурсів C та часу T:

$$Э_{SP}(U_{SP}) = F(Э_f(U_{SP}), Э_\rho(U_{SP}), Э_\tau(U_{SP})).$$

Діяльність із захисту інформації містить адміністративну, процедурну та технічну складові. Виходячи з цього, ми можемо розглядати ефективність управління захистом інформації Y_{man} (ефективність системи управління захистом інформації), ефективність організації захисту інформації Y_{op} (ефективність організаційної системи захисту інформації) та ефективність технічних систем у захисті інформації Y_{tech}. Для кожної з цих видів ефективності цілком логічно розглядати функціональну, економічну та часову ефективності (рис. 2).

У галузі захисту інформації досить глибокий розвиток знайшли питання ефективності технічних, криптографічних, фізичних систем захисту, комплексів, механізмів та способів захисту інформації, що відповідає сучасному розвитку методологічних підходів до захисту інформації. Останнім часом у роботах фахівців, у міжнародних та національних стандартах піднімаються питання управління захистом інформації, починають формулюватися задачі в сфері ефективності управління захистом інформації. Але питання ефективності діяльності із захисту інформації, питання раціональної організації цієї діяльності поки що не знайшли відповідного відображення у сучасних роботах з теорії захисту інформації.

3. ЗРІЛІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ

Зрілість захисту інформації об'єднує множину властивостей які охоплюють аспекти розвитку, еволюції захисту інформації, як діяльності, характеризують функціональні можливості організаційної системи захисту інформації.

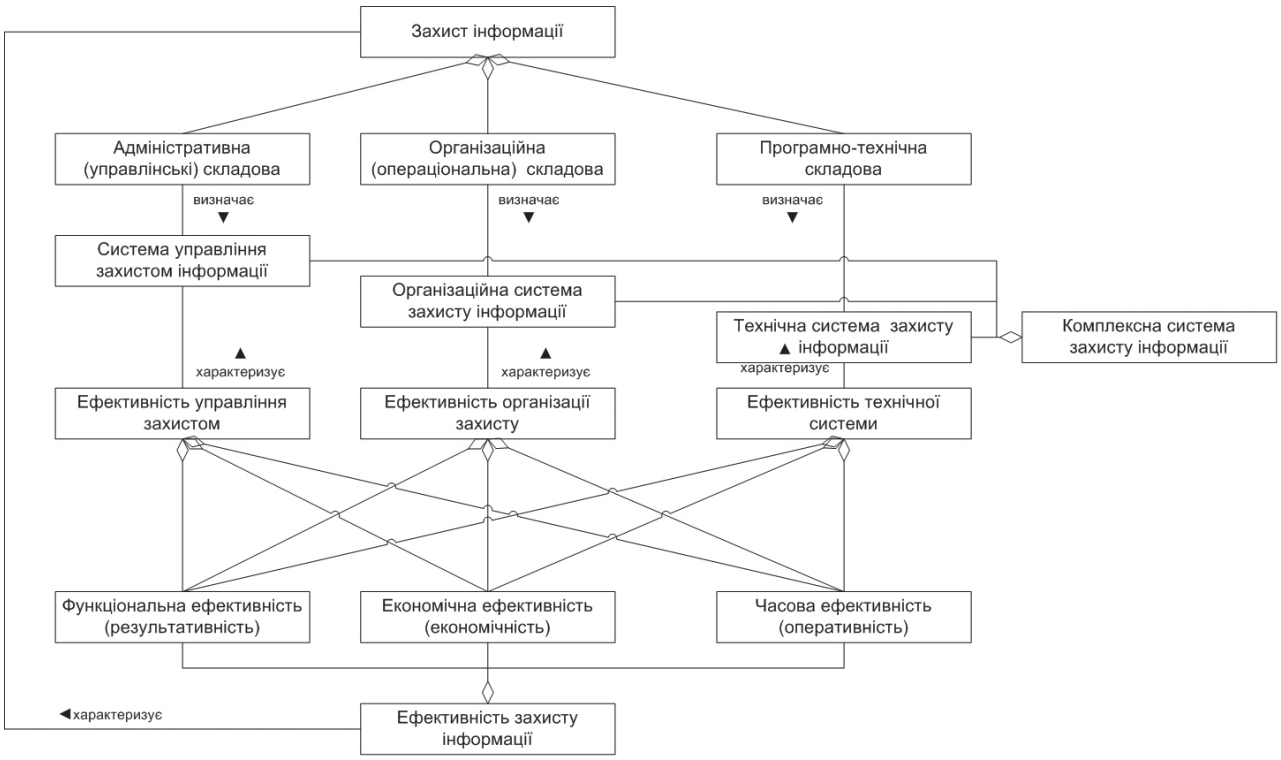

Рис. 2. Проблемно-орієнтовна онтологія ефективності захисту інформації

4. АДЕКВАТНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ

Під *адекватністю* захисту інформації розумітимемо співвідношення рівня функціональної ефективності захисту інформації та рівня небезпеки (ризику) інформаційним активам та іншим ресурсам, що пов'язані з обробкою інформації:

$$A = F_A(\text{Э}_f, R).$$

Адекватність визначає, що даний рівень безпеки інформації L_{SI} дійсно відповідає ситуації, яка склалася відносно існуючих загроз та рівня ризиків безпеці і задовольняє потреби власника інформаційних ресурсів відносно забезпечення безпеки інформації. Захист інформації є адекватним, якщо правила безпеки, рівень зрілості процесів захисту інформації, рівень суворості заходів захисту, рівень гарантій (довіри) захисту інформації, механізми захисту інформації та рівень їх реалізації є адекватними загрозам та ризикам безпеки для певного об'єкта захисту.

5. ПРИЙНЯТНІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ

Прийнятність пов'язана з визначенням несуперечливості задач і цілей захисту інформації місії та загальним цілям організації (об'єкта захисту).

Нехай цілі та задачі захисту інформації будуть подані у вигляді вектора $G_{SI} = \left\{g_1^{SI}, g_2^{SI} \ldots g_n^{SI}\right\}$, а загальні цілі організації у вигляді вектора $G_S = \left\{g_1^S, g_2^S \ldots g_m^S\right\}$. Тоді під прийнятністю захисту інформації розумітимемо ступінь відповідності цілей та задач захисту інформації G_{SI} цілям (місії) G_S організації, у якій здійснюється діяльність із захисту інформації та яка характеризується коефіцієнтом прийнятності виду:

$$K_{accept} = F_{accept}\{G_{SI}, G_S\},$$

де F_{accept} – оператор визначення узгодженості (несуперечливості) цілей захисту та загальних цілей. Таку функцію можна використовувати, наприклад, як неформальні методики цільового аналізу, онтологічного аналізу тощо. Коефіцієнт K_{accept} може бути виражений, наприклад, як лінгвістична змінна рівня узгодженості.

Оцінка прийнятності уточнює питання, чи необхідні цілі і задачі захисту у конкретній організаційній системі, чи не має протиріччя між загальними задачами, що стоять перед нею? Для оцінки захисту інформації за даним критерієм необхідно врахувати усі показники одночасно, виразити відношення між їхніми кількісними формами. Використання для проектування захисту інформації стандартів безпеки або залучення до розв'язання задач захисту експертів – це один з основних доводів прийнятності захисту інформації. Таким чином, захист інформації є прийнятним, якщо цілі і задачі захисту не мають протиріч між місією та основними задачами організації (об'єктів захисту), узгоджені з цілями функціонування організації.

6. ГНУЧКІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ

Гнучкість системи це властивість системи, що полягає у можливості її удосконалення, розширення та надання їй нових якостей [5]. Гнучкість передбачає легку, тобто без великих зусиль та витрат, та достатньо швидку зміну стану системи. Гнучкість, як властивість комплексної системи захисту інформації (КСЗІ), була розглянута у роботі [6]. Інтенсивна зміна середовища безпеки (оточення), умов здійснення діяльності із захисту

інформації призводить до того, що організаційна система захисту інформації (ОСЗІ) має пристосовуватися (адаптуватися) до розв'язання нових задач захисту, що володіють певним ступенем різноманіття. Гнучкість, як економічна категорія відображає здатність ОСЗІ змінювати свої цілі без суттєвих витрат [6]. Спираючись на результати, що отримані у [6] пропонується ввести показник гнучкості ЗІ у вигляді:

$$K_{flex}(t_н,t_к)=\frac{I_{obj}(t_н,t_к)}{I\varsigma(t_н,t_к)},$$

де $K_{flex}(t_н,t_к)$ – гнучкість захисту інформації у період $(t_н,t_к)$; $I_{obj}(t_н,t_к)$ – індекс, що характеризує зміну ступеню різноманітності задач захисту, що розв'язується КСЗІ у період $(t_н,t_к)$; $I\varsigma(t_н,t_к)$ – індекс, що характеризує зміну зведених економічних витрат, що пов'язані із захистом інформації у період $(t_н,t_к)$. Чим більше значення $K_{flex}(t_н,t_к)$, тим захист інформації є більш гнучким.

Гнучкість (реагувальність) пов'язано з оцінкою рівня можливостей (здатності) задовольнити потреби власника інформаційних ресурсів у відношенні безпеки інформації в умовах обстановки, що змінюються, під час здійснення діяльності із захисту інформації та реалізації процесів захисту. Показник гнучкості залежить від індексу зміни ступеня різноманіття задач захисту $I_{obj}(t_н,t_к)$. Серед чинників, що впливають на цей індекс можна виділити такі:

– ступінь варіативності цілей функціонування надсистеми (наприклад бізнес-цілей, цілей автоматизованого управління військами тощо), до якої входить КСЗІ як інтегрована частина.

– варіативність оточення безпеки. Мінливість оточення складається з можливості зміни ресурсів зловмисника, що у свою чергу призводить до зміни кількісного та якісного складу загроз безпеки, зміни ресурсів, що захищаються, сукупність яких визначається з ситуації, що склалася.

Таким чином, захист інформації має бути здатним адекватно реагувати на зміни умов функціонування організації, на зміни цілей і задач функціонування, інтересів і потреб власника інформаційних ресурсів. Захист інформації називається гнучким, якщо він здатний задовольнити потреби у безпеці інформації у будь-яких умовах функціонування організації.

7. ЗДІЙСНЕННІСТЬ ЗАХИСТУ ІНФОРМАЦІЇ

Здійсненність пов'язана з визначенням здійсненності конкретних процесів захисту інформації P у конкретних умовах $X=\{x_1,x_2,...,x_n\}$ при заданих обмеженнях $Y=\{y_1,y_2,...,y_n\}$ у конкретній організації S_0. Необхідно враховувати умови здійсненності захисту інформації і впровадження процесів захисту інформації на різних рівнях забезпечення безпеки інформації. Безпека інформації забезпечується на чотирьох рівнях – законодавчому (правовому), адміністративному, процедурному і програмно-технічному.

На правовому рівні необхідно оцінювати процеси захисту інформації з точки зору їх легітимності. Чи можуть конкретні процеси захисту інформації бути реалізовані на даному об'єкті з точки зору правового поля держави в галузі захисту інформації? Чи має право керівництво приймати такого роду рішення? Чи відповідають положення політики безпеки нормам законів та інших нормативних актів у галузі захисту інформації.

Здійсненність процесів захисту інформації на адміністративному рівні залежить від ступеня розуміння керівництвом цілей безпеки і задач захисту, усвідомлення реальності загроз безпеці, реалізація яких може нанести збиток, рівня сформованості потреб у розв'язанні таких задач захисту.

На процедурному рівні здійсненність процесів захисту інформації залежить від ступеня технологічної і організаційної готовності об'єкта інформатизації до їх впровадження. Тут важливе місце набуває готовність персоналу виконувати конкретні роботи та завдання. Така готовність залежить від багатьох чинників: розуміння персоналом необхідності виконання вимог безпеки, рівень усвідомлення і дисциплінованості персоналу, рівень його професійної підготовленості.

На програмно-технічному рівні на здійсненність процесів захисту інформації має вплив можливість закупівлі необхідних засобів захисту і технічні можливості їх застосування на об'єкті інформатизації, розмір фондів, що виділяються на реалізацію програми забезпечення безпеки інформації і планів захисту, наявність на ринку відповідних засобів захисту потрібної якості, технологічний рівень процесів обробки інформації на об'єкті інформатизації (стан парку обчислювальної та іншої спеціалізованої техніки, рівень комп'ютеризації та інформатизації технологічних процесів і т.ін.).

Враховуючи вищенаведене пропонується ввести до розгляду коефіцієнт здійсненності захисту інформації у вигляді

$$K_{pract}=F(I^{law}_{pract},I^{man}_{pract},I^{op}_{pract},I^{tech}_{pract}),$$

де I^{law}_{pract} – індекс, що характеризує здійсненність захисту інформації в організації на законодавчо-правовому рівні; I^{man}_{pract} – індекс, що характеризує здійсненність захисту інформації в організації S_0 на адміністративному рівні; I^{op}_{pract} – індекс, що характеризує здійсненність захисту інформації в організації S_0 на процедурному рівні; I^{tech}_{pract} – індекс, що характеризує здійсненність захисту інформації в організації S_0 на програмно-технічному рівні; F – оператор агрегування (формування узагальненого показника).

Таким чином, діяльність із захисту інформації є здійсненною, якщо на правовому, адміністративному, процедурному та програмно-

технічному рівнях забезпечення безпеки інформації створено всі умови для здійснення процесів захисту інформації.

8. ПРОСТОТА В АДМІНІСТРАТИВНОМУ ЗАБЕЗПЕЧЕННІ ЗАХИСТУ ІНФОРМАЦІЇ

Властивість *простоти* в адміністративному забезпеченні характеризує діяльність із захисту інформації з точки зору її придатності для адміністрування, тобто враховує наявність достатнього адміністративного ресурсу для реалізації процесів захисту інформації та впровадження політики безпеки, рівень професіоналізму, організаторських здібностей та навичок персоналу управління, що відповідає за організацію ефективного захисту інформації. Діяльність із захисту інформації є простою в адміністративному забезпеченні, якщо вона потребує мінімальних витрат на організаційно-штатні зміни в структурі організації.

ВИСНОВКИ

Таким чином, у рамках системодіяльнісної методології, захист інформації має бути цілеспрямованим, стабільним, безперервним, організованим, керованим, узгодженим та вмотивованим, забезпечувати максимальну ефективність, бути адекватним загрозам та ризикам безпеки, сприйнятим та гнучким в реалізації, здійсненним на різних рівнях забезпечення безпеки інформації, достатньо простим в адміністративному забезпеченні.

Сформульована у роботі множина властивостей не є вичерпною. Але її можна вважати ядром, на основі якого необхідно продовжувати дослідження щодо визначення аналітичних виразів відповідних показників та критеріїв оцінки властивостей, виявлення характеру взаємного впливу властивостей, розробки відповідного науково-методичного апарату оцінювання.

Література

[1] Надежность и эффективность в технике: Справочник: В 10 т./ Ред. Совет: В.С. Авдуевский и др. Т.3. Эффективность технических систем. – М.: Машиностроение, 1988 – 382 с.

[2] *Бинкин Б.А.* Эффективность управления: наука и практика. – М.:Наука, 1982.

[3] Эффективность торговли: сущность, измерение, оценка. – К.:Вища школа, 1986. – 32 с.

[4] *Маркіна І.А.* Методологічні питання ефективності управління // Фінанси України. – 2000. – №6. – С. 24-32.

[5] *Першиков В.И.*, *Савинков В.М.* Толковый словарь по информатике. – М.: Финансы и статистика, 1991.

[6] *Скрипник Л.В.*, *Потий А.В.* Гибкость и специализация профиля защиты автоматизированной системы. // Радиотехника. Всеукраинский межвед. Научн.-техн. Сб. – 2001. – Вып. 119. – С. 17-21.

Надійшла до редколегії 7.04.0.2012

Потій Олександр Володимирович, професор, доктор техн. наук, начальник кафедри радіоелектронних систем пунктів управління Повітряних Сил ім. І. Кожедуба. Область наукових інтересів: проектування комплексних систем захисту інформації, системний аналіз процесів захисту інформації, управління захистом інформації.

Пилипенко Дмитро Юрійович, аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: управління процесами захисту інформації.

Гладкий Дмитро Іванович, молодший науковий співробітник науково-дослідної лабораторії системних технологій ХНУРЕ. Область наукових інтересів: аналіз ризиків, проблеми забезпечення безпеки інформації в ІТС.

УДК 681.3.06

Свойства деятельности по обеспечению защиты информации как системной категории / А.В. Потий, Д.Ю. Пилипенко, Д.И. Гладкий // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 299–303.

В работе исследуются свойства деятельностного аспекта защиты информации как системной категории. Сформированное множество свойств позволяет проводить всестороннюю оценку деятельности по обеспечению защиты информации. Данное множество свойств представляет определенную основу для дальнейших исследований и разработки аналитических выражений и критериев оценки системы защиты информации в организации.

Ключевые слова: системодеятельностный подход, деятельность по обеспечению защиты информации, оценивание.

Ил. 02. Библиогр.: 06 назв.

UDC 681.3.06

The properties of information security activities as a system category / A.V. Potiy, D.Yu. Pilipenko, D.I. Gladkiy // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 299–303.

The properties of information security activities as a system category are studied. The proposed set of properties enables a comprehensive evaluation of information security activities. The given set of properties can be considered as the basis for further research and development of analytical forms and criteria for IS system evaluation in an organization.

Keywords: system-structural approach, information security activities, evaluation.

Fig. 02. Ref.: 06 items.