МЕТОДИ ПОСИЛЕННЯ БЕЗПЕЧНОСТІ IP ПРОТОКОЛІВ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ ГНУЧКИХ КРИТЕРІЇВ БЕЗПЕКИ

УДК 004.3(075)

ВЕСЕЛОВСЬКА Галина Вікторівна
к.т.н., доцент кафедри інформаційних технологій Херсонського національного технічного університету.
Наукові інтереси: технології підвищення ефективності комп'ютерних систем і мереж.
e-mail: galina.veselovskaya@gmail.com

БАРАНЕНКО Роман Васильович
к.т.н., доцент кафедри інформаційних технологій Херсонського національного технічного університету.
Наукові інтереси: геоінформаційні та інформаційно-вимірювальні системи, захист інформації.
e-mail: scrooger@yandex.ua

ДЕРЕВ'ЯНКО Євгеній Іванович
студент спеціальності 8.05010201 «Комп'ютерні системи та мережі» Херсонського національного технічного університету.
Наукові інтереси: технології підвищення ефективності комп'ютерних систем і мереж.

ВСТУП

Специфіка сучасного стану теорії та практики захисту комп'ютерних систем і мереж, діючих на їх платформі інформаційних систем тощо (надалі скорочено – КСМ) від несанкціонованих дій полягає у тому, що питання забезпечення належного рівня безпеки зазначених систем мають ставитися та вирішуватися не тільки на предпроектній стадії та в процесі проектування, а й протягом усього їх життєвого циклу. Необхідність систематичного та всебічного дослідження та відповідного вдосконалювання систем захисту КСМ від несанкціонованих дій обумовлюється необхідністю урахування як існуючої передісторії, поточної статистики та прогнозних тенденцій виникнення загроз, так і ряду інших численних передбачуваних і непередбачуваних факторів, які виявляються вже у процесі реальної роботи системи.

Одну з найважливіших, найопрацьованіших і, разом із тим, досі найуразливіших ланок КСМ щодо впливів несанкціонованих дій являють собою IP протоколи комп'ютерних мереж. Відповідно, актуальною задачею забезпечення належного рівня безпечності КСМ на рівні IP протоколів комп'ютерних мереж є досягнення високого рівня ефективності досліджень IP протоколів комп'ютерних мереж за критеріями безпеки протягом усіх етапів життєвого циклу зазначених систем. Представлені у даній публікації розробки надають ряд підходів, які доповнюють існуючі технології розв`язування вказаної задачі ([1-7] та ін.).

ПОСТАНОВКА ЗАДАЧІ

Здійснювані авторами аналіз і розробка концепцій, методів і моделей посилення безпечності IP протоколів комп'ютерних мереж на основі підвищення ефективності їх досліджень за критеріями безпеки, обумовили необхідність декомпозиції загальної задачі на ряд наступних підзадач: 1) розробка узагальненої концептуальної моделі вирішення проблеми створення передумов для підвищення безпечності IP протоколів комп'ютерних мереж на етапі їх дослідження за критеріями безпеки; 2) розробка методу та моделей підвищення інформативності дослідження IP протоколів комп'ютерних мереж за критеріями безпеки; 3) розробка методу моделювання моніторингу й аналізу стану безпечності

деяких типових категорій легітимних користувачів стосовно здійснення несанкціонованих дій на рівні порушення критеріїв безпеки IP протоколів комп'ютерних мереж; 4) розробка моделі показника безпеки на рівні IP протоколів комп'ютерних мереж із урахуванням підвищеної деталізації дослідження деяких типових категорій легітимних користувачів. У даній статті буде розглянуто підзадачі 1, 3 і 4, а також додатково опрацьовано підзадачу 2, основні підходи до розв'язування якої було запропонованої авторами в рамках публікації [8].

РОЗВ'ЯЗОК ЗАДАЧІ

Розглянемо першу з поставлених вище підзадач, яка полягає в розробці узагальненої концептуальної моделі вирішення проблеми створення передумов для підвищення безпечності IP протоколів комп'ютерних мереж на етапі їх дослідження за критеріями безпеки.

У підсумку вивчення теорії та реальної практики застосування мережних протоколів, було виявлено, що на сьогодні фактичним є стан недостатнього рівня безпечності IP протоколів комп'ютерних мереж, що вимагає пошуку шляхів його підвищення. Подальше деталізоване дослідження питань відповідності IP протоколів комп'ютерних мереж критеріям безпеки дозволило виявити резерви її посилення на шляху вирішення проблеми підвищення ефективності досліджень IP протоколів комп'ютерних мереж за критеріями безпеки. Згідно з вище сказаним, у рамках теми даного розгляду, буде здійснено аналіз визначальних особливостей і постановку актуальних підпроблем загальної проблеми дослідження IP протоколів комп'ютерних мереж за критеріями безпеки.

Насамперед відзначимо, що проведений у процесі роботи над розв`язуванням даного завдання аналіз сучасного стану справ у галузі забезпечення безпеки комп'ютерних систем і мереж на рівні IP протоколів, дозволяє у цілому зробити два наведених нижче ключових висновки.

По-перше, початкова проблема дослідження IP протоколів комп'ютерних мереж за критеріями безпеки може бути розшарована на ряд окремих, відносно самостійних актуальних підпроблем, вирішення яких можливо здійснювати достатньо автономно одна стосовно одної.

По-друге, з метою забезпечення належної дієвості вирішення проблеми дослідження IP протоколів комп'ютерних мереж за критеріями безпеки у реальній практиці роботи, як правило, зазначену узагальнену проблему доцільно зводити до набагато локальніших проблем дослідження безпечності певних реалізацій систем захисту конкретних комп'ютерних систем і мереж на рівні IP протоколів.

Проаналізуємо ряд найважливіших аспектів, пов'язаних із наведеними вище висновками, детальніше.

У першу чергу відзначимо, що специфікаціям IP протоколів комп'ютерних мереж властиві певні характерні особливості, пов'язані з закладеними до указаних протоколів на етапі їх створення та подальшого розвитку концепціями та механізмами, що об'єктивно обумовлюють відповідні потенційно можливі види уразливості IP протоколів комп'ютерних мереж щодо несанкціонованих дій.

Також важливо відзначити, що для IP протоколів комп'ютерних мереж початково була характерною проблема відсутності власних (убудованих) механізмів безпеки, яку не змогла вичерпно вирішити поява додаткового протоколу IPSec стеку протоколів TCP/IP, удосконаленої версії IP протоколу IPv6 та інші подібні заходи. Наявність зазначеної проблеми обумовила необхідність забезпечення IP протоколів комп'ютерних мереж додатковими методами та засобами безпеки, застосовуючи для їх інтеграції системотехнічні підходи.

Разом із тим, існуючі методи, засоби та системи захисту на рівні IP протоколів комп'ютерних мереж, спрямовані на подолання характерних уразливостей безпеки зазначених протоколів, теж не позбавлені певних уразливостей, виявлення кожної з яких стає стимулом для подальшої роботи щодо вдосконалювання інструментарію захисту.

Таким чином, відповідність рівня захищеності IP протоколів комп'ютерних мереж критеріям безпеки можна інтерпретувати як певну систему функціональних залежностей, аргументами яких є показники ефективності систем захисту зазначених протоколів, спрямованих на подолання наявних і потенційно можливих уразливостей їх безпеки.

Проаналізуємо детальніше ще один аспект поставленої проблеми.

Існуючі загальноприйняті нормативні та додаткові системи критеріїв безпеки комп'ютерних систем і мереж, мережних протоколів і, зокрема, IP протоколів, мають за основну мету визначення належності конкретних об'єктів захисту вказаних вище категорій до одного з глобальних класів безпеки. Природно, що вказані критерії безпеки є дуже узагальненими й достатньо інерційно поновлюваними, що не дозволяє так само ефективно застосовувати їх до розв'язування ряду інших задач забезпечення безпеки. Зокрема, для задач отримання дієвих систем захисту, зазначені критерії виявляються недостатньо інформативними.

Таким чином, високу актуальність має задача створення таких додаткових систем критеріїв безпеки, які надавали би можливість достатньо детально й оперативно відображати специфіку стану забезпечення безпеки конкретних об'єктів захисту.

Слід також відзначити один із найпроблемніших аспектів забезпечення безпеки комп'ютерних систем і мереж на рівні IP протоколів, якому на даний час приділяється неналежно мало уваги й яким є користувач. Навіть легітимний користувач може стати потенційним джерелом дуже серйозної небезпеки, якщо його дії (з будь-яких причин) почнуть відноситися до категорії непередбачуваних. Зокрема, непередбачуваність поведінки легітимного користувача може зробити марними як усі зусилля з посиленого шифрування інформації, каналів зв'язку, так і будь-які інші заходи. Виходячи з вище сказаного, важливим кроком є посилення уваги до моделювання поведінки користувачів як ланок систем забезпечення безпеки на рівні IP протоколів під кутом зору моніторингу, прогнозування й управління стабільністю зазначеної поведінки.

У цілому, проблема дослідження IP протоколів комп'ютерних мереж за критеріями безпеки передбачає вирішення множини актуальних підпроблем, представленої концептуально-структурною моделлю

$$П=\{ПДСУ, ПЗСМ, ПК, ПЗСК\}, \quad (1)$$

де:

– ПДСУ – дослідження специфічних уразливостей безпеки IP протоколів комп'ютерних мереж на більш поглибленому рівні, з акцентуванням уваги на питанні максимальної вичерпності виявлення можливих передумов виникнення зазначених уразливостей;

– ПЗСМ – дослідження загального стану методів, засобів і систем захисту IP протоколів комп'ютерних мереж щодо можливостей забезпечення ними належної відповідності зазначених протоколів критеріям безпеки, наявності уразливостей, пошуку резервів удосконалювання шляхом модифікації й інтеграції існуючих підходів, створення нового інструментарію тощо;

– ПК – дослідження користувачів як ключових складових елементів систем забезпечення безпеки IP протоколів комп'ютерних мереж на рівні моделювання об'єктів і процесів моніторингу, прогнозування й управління стабільністю їх поведінки;

– ПЗСК – дослідження загального стану систем критеріїв безпеки IP протоколів комп'ютерних мереж стосовно можливостей підвищення рівня їх інформативності.

Таким чином, у даному розглядяді було здійснено постановку ряду актуальних підпроблем загальної проблеми дослідження IP протоколів комп'ютерних мереж за критеріями безпеки та побудовано відповідну концептуально-структурну модель.

Другу з поставлених вище підзадач, яка полягає в розробці методу та моделей підвищення інформативності дослідження IP протоколів комп'ютерних мереж за критеріями безпеки, було початково розглянуто в публікації [8], де було представлено наступні результати:

– ключові складові вихідних версій моделей базисних множин додаткових критеріїв безпеки IP протоколів, підтримуваних на засадах використання перспективних технологій моделювання та прогресивного спеціалізованого програмного забезпечення;

– метод підтримки здійснення конкретизованих програмних реалізацій додаткових систем критеріїв безпеки, що мають виконувати роль індикаторів повномасштабності та комплексності використання перспективних методів і засобів підтримки безпеки IP протоколів, оснований на застосуванні трьох послідовних рівнів деталізації значень критеріїв;

– формалізований опис загальної моделі структури набору значень тих критеріїв, які відіграють роль

індикаторів для потенційно підтримуваного рівня безпеки IP протоколів;

– рекомендації щодо створення динамічно поновлюваної інтелектуалізованої інформаційної системи з дослідження IP протоколів комп'ютерних мереж за критеріями безпеки.

Виходячи з розробок і позначень, представлених у [8], інтегрований числовий критерій індикації потенційно підтримуваного рівня безпеки IP протоколів IC набуде вигляду наступної функціональної залежності:

$$IC = fIC(< fl(i,j), nm(i,j), cf(i,j), ac(i,j), im(i,j) >), \quad (2)$$

де [8]:

– i, j є номерами конкретних груп та елементів груп, а t(i,j) є найменуваннями для додаткових критеріїв безпеки IP протоколів, відповідних тим перспективним технологіям захисту, що потрібні для здійснення найбільш повних і комплексних підходів;

– fl(i,j), nm1(i,j), nm2(i,j), cf1(i,j), cf2(i,j), sf1(i,j), sf2(i,j), ac1(i,j), ac2(i,j), im1(i,j), im2(i,j) є мірами успішності втілення додаткових критеріїв безпеки IP протоколів щодо певних умов і систем захисту, що відображають аспекти інформативності й одиниць виміру;

– fl(i,j) Є {0, 1} відображає факти реалізованості конкретних критеріїв безпеки IP протоколів t(i,j);

– (nm1(i,j), nm2(i,j)) є узагальненими мірами реалізованості критеріїв безпеки IP протоколів t(i,j), що включають дві узгоджені між собою експертні оцінки (лінгвістичну nm1(i,j) та числову nm2(i,j));

– (cf1(i,j), cf2(i,j)), (sf1(i,j), sf2(i,j)), (ac1(i,j), ac2(i,j)), (im1(i,j), im2(i,j)) є мірами реалізованості глобальних критеріїв безпеки IP протоколів (конфіденційності, цілісності, доступності й імітостійкості), підтримуваними завдяки спрацьовуванню конкретних додаткових критеріїв безпеки IP протоколів t(i,j), які передбачають належні лінгвістичні та числові експертні оцінки.

Задача оптимізації полягатиме в отриманні максимального рівня безпеки IP протоколів IC як функції від fl(i,j) та nm2(i,j) за наступних умов:

– при дотриманні одиничного значення fl(i,j);

– при враховуванні нижньої межі значень nm2_min для nm2(i,j);

– при забезпеченні максимальних значень cf2(i,j), sf2(i,j), ac2(i,j) та im2(i,j);

– при мінімізації інкременту витратності системи захисту dv та декременту продуктивності системи dp, у рамках заданих верхніх меж їх значень dv_max, dp_max.

Тобто ключова математична модель задачі оптимізації для поставленої вище проблеми набуде наступного вигляду:

$$\begin{gathered} IC\_optim = \max IC (< fl(i,j), nm2(i,j), cf2(i,j), sf2(i,j), \\ ac2(i,j), im2(i,j) >), \\ fl(i,j) = 1, nm2(i,j) >= nm2\_min, dv <= dv\_max, dp \\ <= dp\_max, \\ cf2(i,j) -> max, sf2(i,j) -> max, ac2(i,j) -> max, im2(i,j) \\ -> max, \\ dv -> min, dp -> min. \end{gathered} \quad (3)$$

Таким чином, у даному розгляді було доопрацьовано запропонований у [8] новий актуальний метод побудови додаткової системи критеріїв безпеки IP протоколів комп'ютерних мереж, заснований на використанні гнучкого динамічного підходу та сучасних інформаційних технологій, із поданням відповідних концепцій і моделей; застосування удосконаленого методу надає можливість додатково підвищити рівень інформативності дослідження безпечності IP протоколів комп'ютерних мереж.

Розглянемо третю з поставлених вище підзадач, яка полягає у розробці методу моделювання моніторингу й аналізу стану безпечності деяких типових категорій легітимних користувачів стосовно здійснення несанкціонованих дій на рівні порушення критеріїв безпеки IP протоколів комп'ютерних мереж

Легітимні користувачі являють собою той аспект систем безпеки на рівні IP протоколів комп'ютерних мереж, якому традиційно приділялося неналежно мало уваги. Основний підхід полягав у тому, що легітимний користувач розглядався як такий, що є стабільно безпечним і за визначенням не може здійснювати будь-які несанкціоновані дії.

Натомість легітимний користувач може у будь-який момент часу стати джерелом достатньо небезпечних несанкціонованих дій, виконуючи їх найрізноманітнішими способами: свідомо або неусвідомлювано; завчасно готуючися або спонтанно;

пасивно або з високим ступенем зацікавленості у досягненні певного результату, активності й ініціативності; без надання для здійснення несанкціонованих дій спеціалізованих засобів і заходів або надаючи для них усю необхідну інформаційну, технічну та технологічну підтримку; керуючи їх організацією та реалізацією або безпосередньо здійснюючи їх тощо.

Тому важливим є якомога детальніше сумісне вивчення наступних двох ключових аспектів: рівня безпечності легітимних користувачів під кутом зору зрізу його поточного стану на певний момент часу; динаміки змінювання рівня безпечності зазначених користувачів, зі здійсненням ретроспективного та перспективного (прогнозного) аналізу наявної статистики.

Різні категорії легітимних користувачів мають суттєво різні властивості щодо можливостей моніторингу їх безпечності. Значну за загальним обсягом, а тому дуже важливу для ретельнішого розгляду категорію легітимних користувачів становлять ті з них, робота яких на базі інформаційних систем здійснюється на постійній основі, маючи регулярний характер. Зазначена категорія легітимних користувачів дозволяє підтримувати достатньо систематичний і детальний моніторинг та аналіз їх безпечності на всіх етапах їх роботи з системою.

У першу чергу, інтерес представляє множина видів моделей моніторингу та аналізу безпечності легітимних користувачів стосовно здійснення несанкціонованих дій на рівні порушення критеріїв безпеки IP протоколів комп'ютерних мереж, представлена узагальненою структурною моделлю наступного виду:

$$M=\{МО, ММ, МЛ, МСК, МСН\}, \quad (4)$$

Розглянемо призначення складових елементів наведеної вище множини моделей.

МО являє собою модель моніторингу й аналізу стану обізнаності (рівня знань, умінь і навичок) легітимних користувачів і груп користувачів щодо питань безпеки у цілому та, зокрема, відносно володіння теорією та майстерністю безпечної роботи, несприяння несанкціонованим діям і протидії зловмисникам у межах конкретної інформаційної системи та під кутом зору дотримання критеріїв безпеки IP протоколів комп'ютерних мереж.

ММ є моделлю моніторингу й аналізу стану особистої вмотивованості, цілеспрямованості, активності позиції, ініціативності та спланованості дій легітимних користувачів і груп користувачів щодо збереження безпеки в цілому та, зокрема, безпеки конкретної інформаційної системи під кутом зору дотримання критеріїв безпеки IP протоколів комп'ютерних мереж.

МЛ представляє модель моніторингу й аналізу стану психо-фізіологічної лабільності легітимних користувачів і груп користувачів стосовно провокаційних впливів із боку зловмисників у цілому та, зокрема, стосовно безпеки конкретної інформаційної системи під кутом зору дотримання критеріїв безпеки IP протоколів комп'ютерних мереж.

МСК позначає модель моніторингу й аналізу стану схильностей легітимних користувачів і груп користувачів до тих впливів комунікаційного оточення, що можуть призводити до підбурення їх на здійснення несанкціонованих дій або пасивне сприяння ним, у цілому та, зокрема, стосовно безпеки конкретної інформаційної системи під кутом зору дотримання критеріїв безпеки IP протоколів комп'ютерних мереж.

МСН є моделлю моніторингу й аналізу стану схильності користувачів і груп користувачів до ненавмисних та умисних несанкціонованих дій, а також до непротидії ним, у цілому та, зокрема, стосовно безпеки конкретної інформаційної системи під кутом зору дотримання критеріїв безпеки IP протоколів комп'ютерних мереж.

Моніторинг безпечності легітимних користувачів доцільно здійснювати неперервно протягом усіх основних етапів взаємодії користувачів із системою, забезпечуючи посилення контролю за станом і діями користувачів як у процесі входу до системи, так і під час роботи в системі (з відповідною диференціацією для виконання функцій різних типів) та виходу з неї.

Виходячи з вище сказаного, доцільним є розгляд питання про побудову основаної на знаннях моделі безпеки легітимного користувача стосовно здійснення несанкціонованих дій на рівні порушення критеріїв безпеки IP протоколів комп'ютерних мереж.

У першу чергу, мова йде про розширення існуючого апарату моделювання прав доступу легітимних користувачів у системі інтелектуальною моделлю безпеки

легітимного користувача, що передбачає формування міток прав доступу легітимних користувачів до об'єктів, процесів тощо на основі інтелектуальних правил.

Реалізація зазначеної моделі передбачає функціонування комплексу додаткових інтелектуальних програм-моніторів, які здійснюють поглиблену перевірку бепечності легітимного користувача на основі інтелектуальної моделі з використанням сучасної інформаційної технології експертних систем.

А саме, дана експертна система має підтримувати наступні дії: здійснювати моніторинг характеристик легітимних користувачів, пов'язаних із визначенням стану їх безпечності щодо несанкціонованих дій на рівні IP протоколів комп'ютерних мереж; виконувати на основі отриманих значень характеристик стану безпечності легітимних користувачів виведення експертних висновків про їх вплив на формування міток прав доступу користувачів у системі.

Таким чином, у даному розгляді було розроблено метод моделювання моніторингу й аналізу стану безпечності деяких типових категорій легітимних користувачів стосовно здійснення несанкціонованих дій на рівні порушення критеріїв безпеки IP протоколів комп'ютерних мереж. В основу даного методу покладено узагальнену структурну модель, представлену множиною видів моделей моніторингу й аналізу безпечності легітимних користувачів стосовно виконання указаних несанкціонованих дій.

Розглянемо четверту з поставлених вище підзадач, яка являє собою розробку моделі показника безпеки на рівні IP протоколів комп'ютерних мереж із урахуванням підвищеної деталізації дослідження деяких типових категорій легітимних користувачів.

Виконаємо створення моделі показника безпеки на рівні IP протоколів комп'ютерних мереж на засадах посиленого моніторингу (а саме, підвищеної деталізації дослідження) легітимного користувача.

З урахуванням акцентування додаткової уваги на факторі легітимного користувача, будемо розглядати модель показника безпеки на рівні IP протоколів комп'ютерних мереж у наступному виді:

$$S = A \circ U = \varphi(< pi >) \circ v(< qj >), \qquad (5)$$

де: $< pi >$, $< qj >$ являють собою кортежі параметрів, значення яких відображають міри відповідних складових множин інтегрованих факторів безпеки Pi (i = 1, ... , N) та Qj (j = 1, ..., M); " ∘ " є позначенням композиції функцій.

Розглянемо призначення факторів множини Pi (i = 1, 2 , 3).

Фактор P1 характеризує цінність збереження безпеки тієї інформації, що підлягає захисту на рівні IP протоколів комп'ютерних мереж, інтегруючи підфактори нормативної передбаченості певного статусу збереження, морально-психологічної значимості, функціональної необхідності та матеріальної вартості зазначеної інформації.

Фактор P2 характеризує важливість збереження, у підсумку впровадження системи захисту на рівні IP протоколів комп'ютерних мереж, ключових властивостей інформаційної системи, інтегруючи підфактори збереження властивостей ергономічності, продуктивності й економічності.

Фактор P3 характеризує можливість здійснення несанкціонованих дій щодо порушення безпеки тієї інформації, що підлягає захисту на рівні IP протоколів комп'ютерних мереж, інтегруючи наступні підфактори: можливості появи потенційно невиключених несанкціонованих дій; можливості здійснення спроб несанкціонованих дій; можливості частково або повністю успішної реалізації несанкціонованих дій.

У свою чергу, фактори множини Qj (j = 1, ..., 5) характеризують важливість досягнення позитивних результатів моделювання згідно з розглянутими раніше моделями МО, ММ, МЛ, МСК і МСН відповідно.

Таким чином, у даному розгляді було створено модель показника безпеки на рівні IP протоколів комп'ютерних мереж із урахуванням підвищеної деталізації дослідження деяких типових категорій легітимних користувачів, в основу якої покладено розробку кортежів специфічних щодо даного випадку інтегрованих факторів безпеки.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

Запропоновано нові актуальні методи та моделі посилення безпечності IP протоколів комп'ютерних мереж на основі підвищення ефективності їх досліджень за критеріями безпеки: узагальнена концептуальна мо-

дель вирішення проблеми створення передумов для підвищення безпечності IP протоколів комп'ютерних мереж на етапі їх дослідження за критеріями безпеки; удосконалений метод і моделі підвищення інформативності дослідження IP протоколів комп'ютерних мереж за критеріями безпеки; метод моделювання моніторингу й аналізу стану безпечності деяких типових категорій легітимних користувачів стосовно здійснення несанкціонованих дій на рівні порушення критеріїв безпеки IP протоколів комп'ютерних мереж; модель показника безпеки на рівні IP протоколів комп'ютерних мереж із урахуванням підвищеної деталізації дослідження деяких типових категорій легітимних користувачів. Застосування вказаних методів і моделей дозволяє додатково підвищити інформативність дослідження безпечності IP протоколів комп'ютерних мереж.

ЛІТЕРАТУРА:

1. Shangin V.F. Informatsionnaya bezopasnost kompyuternyih sistem i setey: Uchebnoe posobie /V.F. Shangin. — M.: ID FORUM, NITs INFRA-M, 2013. — 416 s.
2. Kupriyanov A.O. Obespechenie zaschityi personalnyih dannyih v informatsionnyih sistemah //Program. inzheneriya i inform. bezopasnost. – 2013. – №4. – S.27-34.
3. Malyuk A.A. Perspektivyi razvitiya "oblachnyih" tehnologiy. Informatsionnaya bezopasnost i zaschita personalnyih dannyih v "oblachnoy" srede //Vestn. Nats. issledovat. yader. un-ta "MIFI". – 2013. – T.2, №1. – S.120-124.
4. Partyika T.L. Informatsionnaya bezopasnost: Uchebnoe posobie /T.L. Partyika, I.I. Popov. — M.: Forum, 2012. — 432 s.
5. Petrov S.V. Informatsionnaya bezopasnost: Uchebnoe posobie /S.V. Petrov, I.P. Slinkova, V.V. Gafner. — M.: ARTA, 2012. — 296 s.
6. Prokushev Ya.E. Sravnitelnyiy analiz sredstv programmno-apparatnoy zaschityi informatsii, primenyaemyih v informatsionnyih sistemah personalnyih dannyih /Ya.E. Prokushev, S.V. Ponomarenko //Informatsiya i bezopasnost. – 2012. – T.15, №1. – S.31-36.
7. Razrabotka avtomatizirovannoy sistemyi otsenki zaschischennosti i formirovaniya rekomendatsiy po vyiboru sredstv zaschityi informatsionnyih sistem personalnyih dannyih /V.I. Averchenkov, M.Yu. Ryitov, O.M. Golembiovskaya, E.V. Leksikov //Vestn. kompyuter. i inform. tehnologiy. – 2012. – №11. – S.40-45.
8. Veselovska G.V., Baranenko R.V., Derevyanko E.I. Metod pidvischennya informativnosti doslidzhennya IP protokoliv komp'yuternih merezh za kriteriyami bezpeki //Problemi Informatsiynih tehnologiy. – 2015. – №1 (017). – S.132-137.

Рецензент: *д.т.н., проф. Ходаков В.Є.,*
Херсонський національний технічний університет.