УДК 004.056.5

[1]С.С.Бучик, д.т.н.,
[2]О.К.Юдін, д.т.н.,
[1]Р.В.Нетребко

АНАЛІЗ МЕТОДІВ ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

[1]Житомирський військовий інститут імені С.П. Корольова
[2]Національний авіаційний університет

s_stbu@ukr.net
kszi@ukr.net
netr_rv@ukr.net

Проведено аналіз методів визначення стандартних функціональних профілів захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу. Показано наявність малої кількості представлених методів, які зведені авторами до п'яти: перший – стандартний метод; другий – метод перевірки несуперечності та повноти; третій – метод побудови таксономії; четвертий – метод парето-оптимальних функціональних профілів захищеності; п'ятий – удосконалений метод визначення функціональних профілів захищеності вузлів інформаційно-телекомунікаціної системи дерева ідентифікаторів державних інформаційних ресурсів. Здійснено порівняння їх між собою за такими основними параметрами як: рівень витрат, можливість використання як стандартних, так і нестандартних функціональних профілів захищеності, врахування кваліфікації експертів. Визначені переваги та недоліки по кожному з представлених методів з подальшим формулюванням вимог щодо підвищення ефективності визначення стандартних функціональних профілів захищеності

Ключові слова: *функціональний профіль захищеності; несанкціонований доступ; інформаційно-телекомунікаційна система; експертиза; технічний захист інформації*

Актуальність дослідження

Оцінка захищеності систем стала набувати особливої актуальності в Україні починаючи з двохтисячних років, коли почали з'являтися міжнародні стандарти з управління інформаційною безпекою (ІБ). Кожного дня у світі з'являються нові програмні та апаратні засоби, які дають можливість несанкціонованого доступу (НСД) до інформації. Тому спеціалісти з ІБ багатьох країн світу намагаються протистояти даній проблемі, використовуючи різноманітні засоби та методи. За останні роки було розроблено безліч нормативних документів технічного захисту інформації (НД ТЗІ), спрямованих на захист автоматизованих систем (АС) від НСД. Розглядаючи нормативно-правову базу України в даній галузі, слід відмітити наступні документи: НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806; НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22 із змінами згідно наказу Адміністр-

рації Держспецзв'язку від 28.12.2012 № 806; НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22. Саме вони стали основою для проведення аналізу та подальшого дослідження. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», визначає, що експертна комісія проводить оцінку комп'ютерної системи (КС). Тому є актуальним здійснити аналіз методів визначення стандартних функціональних профілів захищеності (ФПЗ), за допомогою яких здійснюють оцінку захищеності інформаційно-телекомунікаційної системи (ІТС).

Аналіз останніх досліджень і публікацій

Аналіз останніх досліджень і публікацій показав, що головною задачею методів визначення стандартних функціональних профілів захищеності ІТС спирається на провідні дослідження інформаційної безпеки, українські та міжнародні стандарти управління інформаційною безпекою та методиці оцінювання інформаційної безпеки. Питання створення, організації та дослідження процесів функціонування і розвитку систем захисту інформації знайшли своє відображення в працях вітчизняних і закордонних вчених, серед яких Горбенко І.Д., Корченко О.Г., Задірака В.К., Конахович Г.Ф., Грайворонський М.В., Новіков О.М., Шаньгин В.Ф., Юдін О.К. і багато інших. У цих працях розроблено ряд основних теоретичних положень з захисту інформації, методологічних та науково-теоретичних основ побудови систем захисту, оцінки їх ефективності та принципів вибору параметрів для оцінки ефективності. Так в роботі [4] авторами розроблено метод формування ФПЗ від НСД на основі побудови таблиць для визначення необхідності та рівня послуг. В роботі [5] авторами визначені лише певні протиріччя щодо сучасного стану нормативно-правової бази (НПБ) ТЗІ. В роботі [6] розглянуто проблемні питання побудови системи захисту інформації (СЗІ) від НСД та формальна постановка завдання вибору оптимального профілю захищеності. Автором статті в роботі [7] представлена загальна модель формування системи захисту державних інформаційних ресурсів (ДІР), в якій одним із елементів системи управління ІБ ДІР є модель вибору ФПЗ. В роботі [2] розгянуто теоретичні основи визначення стандартних ФПЗ на основі НПБ.

Мета статті

Проведення аналізу методів визначення стандартних функціональних профілів захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу**,** порівняння їх між собою. Врахування усіх переваг та недоліків по кожному з методів. Формулювання вимог щодо підвищення ефективності визначення стандартних функціональних профілів захищеності.

Виклад основного матеріалу

Проблема НСД до ресурсів інформаційних систем загострювалась із розвитком інформаційних технологій і тотального використання інформаційно-телекомунікаційних систем у всіх сферах діяльності суспільства. Розв'язання завдань розробки та вибору відповідних ефективних методів і засобів захисту від НСД, значною мірою залежить від низки чинників, пов'язаних із організацією самого процесу НСД, технічних характеристик системи, тощо [1].

Реалізація загроз НСД здійснюється шляхом атак на ресурси інформаційної системи, а суттєвим чинником впливу на успіх атакуючих дій є рівень уразливості системи, недоліки процесів експлуатації, управління, контролю. Контроль за функціонуванням системи ТЗІ здійснюється з метою визначення й удосконалення стану ТЗІ в органах, щодо яких здійснюється

ТЗІ, виявлення та запобігання порушенням з ТЗІ в інформаційних системах та об'єктах. Здійснюється на основі експертизи. Експертиза може бути первинною, додатковою та контрольною (рис. 1) [1, с. 247].

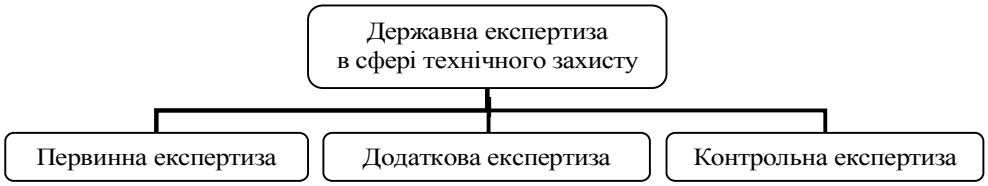

Рис. 1. Класифікація державної експертизи в сфері технічного захисту інформації

Державна експертиза в сфері ТЗІ проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо можливості їх використання для забезпечення технічного захисту інформації. Для проведення експертизи потрібно проаналізувати критерії. Критерії є методологічною базою для визначення вимог з захисту інформації в КС від НСД; створення захищених КС і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в КС і їх придатності для обробки критичної інформації (інформації, що вимагає захисту). З точки зору забезпечення безпеки інформації, можна розглядати як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти деякій множині загроз, які вказані в документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД». Існує певний перелік послуг, які на підставі практичного досвіду визнані «корисними» для забезпечення безпеки інформації. Вимоги до реалізації даних послуг наведені в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД». Вимоги до функціональних послуг розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного з чотирьох основних типів: конфіденційності, цілісності, доступності та спостереженості. Порядок оцінки КС на предмет відповідності цим критеріям визначається відповідними нормативними документами. Експертна комісія, яка проводить оцінку КС, визначає, які послуги і на якому рівні реалізовані в даній КС, і як дотримані вимоги гарантій. Результатом оцінки є рейтинг, що являє собою упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг в критеріях. Для того, щоб до рейтингу КС міг бути включений певний рівень послуги чи гарантій, повинні бути виконані всі вимоги, перелічені в критеріях для даного рівня послуги або гарантій.

Згідно з критеріями, кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз. Для кожної послуги повинна бути розроблена політика безпеки, яка буде реалізована. Політика безпеки має визначати, до яких об'єктів застосовується послуга. Ця визначена підмножина об'єктів називається захищеними об'єктами відносно даної послуги. Множина критеріїв формує ФПЗ – це мінімально необхідний перелік послуг, який може забезпечити СЗІ, щоб задовольнити певні вимоги до необхідного рівня захищеності інформації.

В НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від НСД» та НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від НСД», що призначені для оцінювання функціональних послуг безпеки та описують оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки. Але поза кадром на сьогодні залишилося питання, яким чином первинно обґрунтувати склад ФПЗ. У

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД» визначено підхід до визначення ФПЗ шляхом вибору з множини стандартних ФПЗ. Зважаючи на те, що цей підхід є єдиним, що визначений у НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД» розглянемо його як перший з методів визначення стандартних ФПЗ.

Основними перевагами стандартного методу є відносна простота за рахунок: наявності готових шаблонів ФПЗ для КС, можливості звуження простору вибору за рахунок визначення призначення АС (автоматизації діяльності органів державної влади, автоматизації банківської діяльності, керування технологічними процесами, довідково-пошукові системи), до складу якої входять КС, врахування необхідних зв'язків між послугами, що входять до складу стандартних ФПЗ.

До основних недоліків слід віднести: значну складність (особливо часову) детального аналізу послуг безпеки, що входять до складу стандартних ФПЗ, відсутність формалізованого (та зрозумілого користувачу) зв'язку між включеними до стандартного ФПЗ послугами безпеки (їх рівнями) та загрозами і ризиками для конкретної КС. Власне кажучи, недоліки стандартного методу є наслідком його основної переваги. Стандартний ФПЗ не може повністю відповідати вимогам довільної КС, якщо кількість стандартних ФПЗ не дорівнює загальній кількості можливих ФПЗ, а у випадку рівності цих величин це вже не стандартні ФПЗ, а припустимі профілі. Звісно, що використання у стандартному підході припустимих профілів призвело б до надвеликої складності їх належного аналізу [4].

Авторами у роботі [4] було проаналізовано стандартний метод та показано вимоги до методу: зручність застосування; зрозумілість проміжних результатів та їх впливу на остаточний склад ФПЗ; врахування вимог нормативних документів у сфері ТЗІ; коректність переходів між різними етапи визначення складу ФПЗ; можливість самоперевірки; наявність формалізованого процесу вибору та можливість використання результатів для документування ходу вибору елементів ФПЗ; можливість інтеграції з іншими етапами побудови комплексної системи захисту інформації (КСЗІ).

Даний метод побудований на основі створення таблиць для визначення необхідності та рівня послуг, але на відміну від запропонованої в статті [2] теоретичних основ, він є на думку авторів більш складним та вимагає від особи, що приймає рішення більш детального розуміння змісту та необхідності вимог, також до недоліків слід віднести значну кількість таблиць, що обробляється, значне використання ресурсів та часу.

Також науковцем А. В. Лєншином було запропоновано наступні методи аналізу та побудови функціональних профілів захищеності від НСД: метод перевірки несуперечності та повноти профілю захищеності від НСД [8]; метод побудови таксономії функціональних послуг безпеки від НСД.

При розробці методу перевірки несуперечності та повноти профілю захищеності від НСД висувалися такі вимоги: зручність застосування; зрозумілість проміжних результатів та їх впливу на остаточний склад ФПЗ; врахування вимог нормативних документів; коректність переходів між різними етапи визначення складу ФПЗ; можливість самоперевірки особи, що приймає рішення; наявність формалізованого процесу вибору та можливість використання результатів для документування ходу вибору елементів ФПЗ; можливість інтеграції з іншими етапами побудови
КСЗІ [8].

Основними перевагами цього методу є: прискорення процесу перевірки (результат отримується за хвилину), при цьому процедура верифікації профілю захищеності не висуває вимог до кваліфікації перевіряючого, а лише до його уважності; наочність проміжних та остаточних висновків, що дозволяє сформувати реко-

мендації з корегування складу профілю захищеності.

Основним недоліком, як вважають автори даного методу є те, що не вказується рівень кваліфікації експерта, що приведе до некваліфікованої оцінки рівня безпеки.

При розробці автором А. В. Лєншином методу побудови таксономії функціональних послуг безпеки було вирішено завдання визначення співвідношень, в яких знаходяться рівні послуг безпеки. Як визначено в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД», кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз і може включати декілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Для побудови таксономії послуг безпеки з НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в КС від НСД» було проведено декомпозицію вимог на "елементарні" складові. Подання специфікації послуг безпеки у матричному вигляді дозволило застосувати для її аналізу комбінаторно-морфологічні методи. Зокрема визначити міру включення, що відбиває різну ступінь включення одного об'єкта в інший та дозволяє виявити, який з об'єктів містить більше специфічних властивостей.

Метод побудови таксономії функціональних послуг захисту від НСД має результати, що дозволяють розв'язати завдання з визначення співвідношень, у яких знаходяться послуги безпеки, що є складовими ФПЗ та є передумовою розробки методу, що дозволяє виконати згортку вимог послуг безпеки кількох комплексів засобів захисту (КЗЗ), що входять до складу КСЗІ ІТС.

Відмінною рисою розробленого методу є використання методів системного аналізу та досвіду з розробки КЗЗ, що закріплений у ISO/IEC 15408. Застосування запропонованого методу дозволяє надати можливість розробникам КЗЗ та експертам у сфері ТЗІ обґрунтовано приймати рішення з перевірки та побудови КСЗІ, результати яких мають властивості повторюваності та порівнюваності.

Недоліком даного методу є велика кількість інформації, що обробляється, високий рівень кваліфікації експерта, великі затрати часу та матеріальних ресурсів.

Розроблений метод парето-оптимальних ФПЗ в роботі [3] базується на побудові підмножини, яка для кожної з величин видатків містить лише ті рішення, які дають найкращий рівень захищеності. Перехід від множини можливих рішень до аналізу лише множини, дозволяє наочно представити парето-оптимальні ФПЗ. У такий же спосіб для різних умов функціонування ІТС (різних множин можливих рішень) може бути сформоване ціле сімейство парето-оптимальних ФПЗ, серед яких у подальшому буде обрана як конкретна крива, так й конкретне парето-оптимальне рішення. До недоліків даного методу можна віднести: високу кваліфікацію експерта; відхилення від нормативно-правової бази; велика кількість часу на визначення ФПЗ. До переваг даного методу віднесемо можливість графічного визначення ФПЗ.

Авторами в роботі [2] було запропоновано теоретичні основи визначення стандартних ФПЗ АС від НСД та запропоновано удосконалений метод визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР. Даний метод побудований на основі нормативного документа НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Структурно-логічна схема формалізації визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР представлено на рис. 2.

Перевагами даного методу є автоматизація процесу визначення ФПЗ, середній рівень кваліфікації експерта, можливість швидкого та автоматизованого визначення ФПЗ.

Використання методів перевірки несуперечності та повноти профілю захищеності від НСД, побудови таксономії функціональних послуг безпеки від НСД, парето-оптимальних ФПЗ дає змогу оцінювати систему тільки з боку нестандартних профілів захисту, а стандартні профілі залишаються в стороні, що приводить до невиконання стандартів по критеріях оцінки захисту системи.

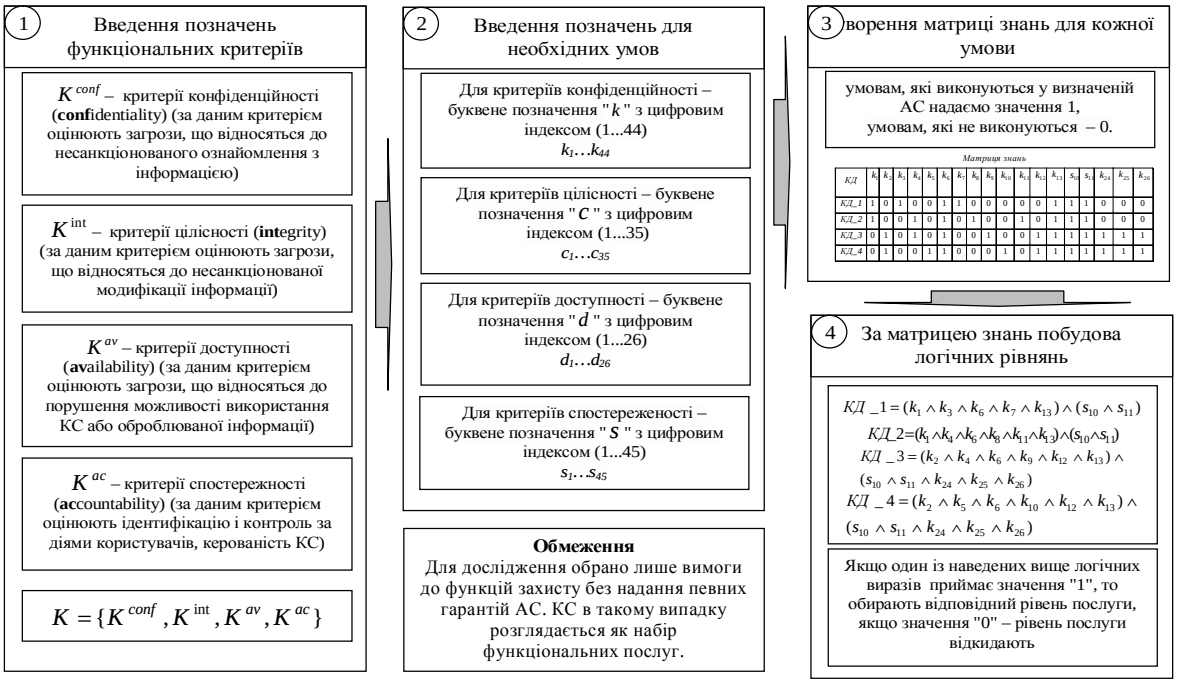

Рис. 2. Структурно-логічна схема формалізації визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР

Також кожний з представлених методів має великі затрати часу та матеріальних ресурсів для їх реалізації, що приводить до нераціонального використання даних методів та потребують високих знань у сфері ФПЗ. Тому актуальним є удосконалення методу формування стандартних ФПЗ, а саме створення програмного продукту визначення ФПЗ автоматизовано. Узагальнений аналіз методів за визначеними параметрами (витратами, можливостями використання стандартних, нестандартних ФПЗ, кваліфікація експерта), які описані вище в статті, представлені в табл. 1.

Таблиця 1. Аналіз методів побудови ФПЗ

Метод побудови ФПЗ	Витрати (рівень)	Використання стандартних ФПЗ	Використання нестандартних ФПЗ	Кваліфікація експерта
Стандартний метод	високий	+	+	середня
Метод перевірки несуперечності та повноти	високий	-	+	висока
Метод побудови таксономії	високий	-	+	висока
Метод парето-оптимальних ФПЗ	високий	-	+	висока
Удосконалений метод визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР	невисокі	+	+	середня

Основні результати

Основними результатами автори вважають здійснення порівняння методів побудови ФПЗ за визначеними параметрами, що надає можливість визначення шляхів подальшого удосконалення стандартного методу за рахунок зменшення витрат на проведення експертизи, можливості використання не тільки стандартних ФПЗ з урахуванням середньої кваліфікації експертів. Запропоновані авторами теоретичні основи в роботі [2] дають можли-

вість в подальшому розробити експертну систему, спираючись на документ НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» в якому визначено підхід до визначення ФПЗ шляхом вибору з множини стандартних ФПЗ, зважаючи на те, що стандартний підхід є єдиним, що визначений у НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

Висновки

Таким чином, у статті проаналізовано методи формування ФПЗ ІТС від НСД. Висвітлено необхідні НД ТЗІ, які регламентують порядок оцінки захищеності інформації від НСД. Визначено, що представлені методи є складними у реалізації і вимагають у експерта значних знань Запропоновані авторами теоретичні основи в роботі [2] та проведений аналіз методів дають можливість в подальшому розробити експертну систему, яка визначатиме стандартні ФПЗ ІТС від НСД. Це полегшить роботу експертів щодо визначення профілю захищеності та створення необхідного комплексу засобів захисту, а також зменшить витрачений ресурс часу.

Список літератури

1. *Юдін О.К.* Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

2. *Юдін О.К.* Теоретичні основи визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу / О.К. Юдін, С.С. Бучик, С.В. Мельник // Наукоємні технології. – 2016. – № 2 (30). – С.195 – 205, doi.org/10.18372/2310-5461.30.10564

3. *Берестов Д.С.* Побудова парето-оптимальних функціональних профілів захищеності / Д.С. Берестов, М.О. Гульков, В.А. Козачок // Збірник наукових праць. Вип. 1(39) / Редкол. Шевченко В. Л. (голова) та ін. – К.: ЦВСД НУОУ, 2009. – С. 89–94. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Znpcvsd/2009_1/12.pdf.

4. *Лєншин А.В.* Метод формування функціональних профілів захищеності від несанкціонованого доступу // А.В. Лєншин, П.В. Буслов. // Радіоелектронні і комп'ютерні системи : науч. тр. – Х.: Нац. аэрокосм. ун-т "ХАИ", 2010. – Вып. 7(48). – С. 77–81. – Режим доступу: http://nbuv.gov.ua/UJRN/recs_2010_7_15.

5. *Паламарчук Н. А.* Сучасний стан нормативно-правової бази в галузі технічного захисту інформації // Н. А. Паламарчук, Ю. І. Хлапонін, В. В. Овсянніков // Збірник наукових праць ВІТІ НТУУ "КПІ" – К.: ВІТІ НТУУ "КПІ", 2011. – №3. – С. 78 – 82. – Режим доступу: http://viti.edu.ua/ files/ zbk/ 2011/ 11_3_2011.pdf.

6. *Шевченко В.Л.* Метод пошуку проектних альтернатив системи захисту інформації // В.Л. Шевченко, Д.С. Берестов // Сучасний захист інформації – К.: ДУТ, 2015. – №3. – С.22 – 27. http://journals.dut.edu.ua/index.php/dataprotect/article/viewFile/386/358

7. *Юдін О.К.* Загальна модель формування системи захисту державних інформаційних ресурсів / О.К. Юдін, С.С. Бучик, О.В. Фролов // Наукоємні технології. – 2015. – № 4 (28). – С.332 – 337, doi.org/10.18372/2310-5461.28.9678

8. *Потій О.В.* Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу /О.В. Потій, А.В. Лєншин //Научно-технический журнал "Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения информационной безопасности". – Х., 2010. – Том 9. – №3. – С.479 – 488. – Режим доступу: http://openarchive.nure.ua/handle/document/410.

Статтю подано до редакції 12.12.2016