УДК 004.056.5

Р. В. Нетребко

АНАЛІЗ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ТА МЕТОДІВ ВИЗНАЧЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

У статті проаналізовано нормативно-правове забезпечення України та розглянуто методи визначення захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу. З'ясовано, за допомогою яких нормативних документів оцінюють рівень захищеності інформаційно-телекомунікаційних систем від несанкціонованого доступу. У результаті аналізу встановлено факт наявності малої кількості потрібних методів та здійснено порівняння їх між собою. Описано переваги та недоліки кожного з подальшим формулюванням вимог щодо підвищення ефективності визначення функціональних профілів захищеності. Сплановано подальші кроки дослідження для оцінювання рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу.

Ключові слова: *нормативно-правове забезпечення, рівень захищеності, інформаційно-телекомунікаційна система, несанкціонований доступ.*

Постановка проблеми в загальному вигляді. Захист інформації є одним із найбільш актуальних напрямків сучасної науки і техніки, що сформовані на базі новітніх технологій. Безпека інформаційних ресурсів надзвичайно важлива в різних галузях, де потрібні зберігання й передача даних для різноманітних інформаційних систем суспільства. Це пов'язано з досить високою комерційною вартістю інформації та постійно зростаючими обсягами потоків даних, які необхідно передавати на великі відстані без втрати або спотворення корисної інформації. Для оцінювання захисту інформації потрібно визначати рівень захищеності. Як і будь-яка організаційна діяльність, цей процес вимагає витрат матеріальних ресурсів (фінансових, трудових). Тому спеціалісти з інформаційної безпеки багатьох країн світу намагаються вирішити дану проблему, використовуючи різноманітні засоби та методи. Звідси постає актуальне питання щодо аналізу нормативно-правової бази (НПБ) та методів визначення рівня захищеності інформаційно-телекомунікаційних систем (ІТС) від несанкціонованого доступу (НСД).

Аналіз останніх досліджень і публікацій показав, що головним завданням методів визначення рівня захищеності ІТС є пошук конкретного функціонального профілю захищеності (ФПЗ). Питання створення, організації та дослідження процесів функціонування й розвитку систем захисту інформації розглянуто 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., Чунарьова А. В., Чунарьов А. В. тощо. Дослідниками розроблено основні теоретичні положення із захисту інформації, методологічні та науково-теоретичні основи побудови систем захисту, оцінювання їх ефективності та принципи вибору параметрів для цього.

Так, у роботі [1] авторами розроблено метод формування ФПЗ від НСД на основі побудови таблиць для визначення рівня послуг. У [2] науковці встановили певні протиріччя щодо сучасного стану НПБ технічного захисту інформації (ТЗІ). У [3] розглянуто проблемні питання побудови системи захисту інформації (СЗІ) від НСД та формальну постановку завдання вибору оптимального профілю захищеності. Автором статті [4] запропоновано загальну модель формування системи захисту державних інформаційних ресурсів (ДІР), у якій одним з елементів системи управління інформаційної безпеки ДІР є модель вибору ФПЗ. У роботі [5] розгянуто теоретичні основи визначення стандартних ФПЗ на основі НПБ.

Формулювання завдання дослідження. Метою статті є аналіз нормативно-правового забезпечення та методів визначення рівня захищеності ІТС від НСД, порівняння їх між собою, врахування усіх переваг та недоліків кожного з них. Формулювання вимог до методу визначення ФПЗ.

Виклад основного матеріалу. Проблема НСД до ресурсів інформаційних систем загострювалася з розвитком інформаційних технологій і тотального використання інформаційно-комунікаційних систем та мереж у всіх сферах діяльності суспільства. Вирішення 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[6].

В Україні розроблено безліч нормативних документів (НД) ТЗІ, спрямованих на захист ІТС від НСД [10]. Вивчаючи НПБ у даній галузі, слід виокремити такі документи:

НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22 зі змінами згідно з наказом адміністрації Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) від 28.12.2012 № 806;

НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22 зі змінами згідно з наказом адміністрації 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», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22;

НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу», затверджений наказом адміністрації Держспецзв'язку від 24.07.2009 № 172;

НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу», затверджений наказом адміністрації Держспецзв'язку від 24.07.2009 № 172 зі змінами згідно з наказом адміністрації Держспецзв'язку від 28.12.2012 № 806.

НПБ НД ТЗІ 2.7-010-09 та НД ТЗІ 2.5-004-99 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 ІТС.

З розглянутої вище НПБ випливає, що в документах НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» та НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу» описано процес оцінювання функціональних послуг безпеки та рівня гарантій коректності їх реалізації, але залишилося питання, яким чином первинно обґрунтувати склад ФПЗ та рівня гарантій. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» встановлює підхід до визначення ФПЗ шляхом вибору з множини стандартних профілів. Даний підхід є єдиним, визначеним у НД ТЗІ. Крім того, в ньому описані критерії оцінки рівня гарантій.

На основі НД ТЗІ 2.5-004-99 було проведено аналіз методів визначення рівня захищеності ІТС, одним з яких є стандартний метод. Його основна перевага –це відносна простота за рахунок: наявності готових шаблонів ФПЗ для ІТС; можливості звуження простору вибору завдяки з'ясуванню призначення ІТС; врахування необхідних зв'язків між послугами, що входять до складу стандартних ФПЗ.

До основних недоліків даного методу слід віднести: значну складність детального аналізу послуг безпеки, передбачених стандартними профілями; відсутність формалізованого зв'язку між включеними до стандартного профілю послугами безпеки та загрозами і ризиками для конкретної ІТС. Стандартний ФПЗ не може повністю відповідати вимогам довільної ІТС, якщо кількість стандартних ФПЗ не дорівнює загальній кількості можливих. А в разі рівності даних величин це вже не стандартні ФПЗ, а припустимі профілі. Звісно, що використання в стандартному підході припустимих профілів призвело б до надвеликої складності їх належного аналізу.

Науковцями А. В. Лєншиним та О. В. Потієм було запропоновано метод побудови таксономії функціональних послуг безпеки та метод перевірки несуперечності й повноти профілю захищеності від НСД [1, 7].

При розробці методу перевірки несуперечності та повноти профілю захищеності від НСД ставилися такі вимоги: зручність застосування; зрозумілість проміжних результатів та їх впливу на остаточний склад ФПЗ; відповідність НД; 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; здатність до інтеграції з іншими етапами побудови комплексної СЗІ.

Даний метод побудований на основі створення таблиць для визначення рівня послуг, але, на відміну від запропонованих у статті [5] теоретичних основ, він є, на думку авторів, складнішим та вимагає від особи, що приймає рішення, більш детального розуміння змісту та необхідності вимог. Крім того, до недоліків слід віднести велику кількість таблиць, що обробляються, а також значне використання ресурсів та часу.

Основними перевагами даного методу є: прискорення процесу перевірки (результат отримується за хвилину), при цьому процедура верифікації профілю захищеності не передбачає вимог до кваліфікації перевіряючого, а лише до його уважності; наочність проміжних та остаточних висновків, що дозволяє сформувати рекомендації з корегування складу профілю захищеності.

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

При розробці А. В. Лєншиним методу побудови таксономії функціональних послуг безпеки було вирішено завдання визначення співвідношень рівнів послуг безпеки. Як визначено в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», кожна послуга – це набір функцій, що дозволяють протистояти певній множині загроз, вона може включати декілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте вони не обов'язково є точною підмножиною один одного. Для побудови таксономії послуг безпеки з НД ТЗІ 2.5-004-99 було проведено декомпозицію вимог на «елементарні» складові. Подання специфікації послуг безпеки в матричному вигляді дозволило застосувати для її аналізу комбінаторно-морфологічні методи, зокрема визначити міру включення, що відображає різний ступінь включення одного об'єкта в інший та дозволяє виявити, який з них має більше специфічних властивостей.

Перевагами запропонованого методу є можливість розробникам комплексних засобів захисту та експертам у сфері ТЗІ обґрунтовано приймати рішення з перевірки та побудови ІТС, результати яких мають властивості повторюваності та порівнюваності.

Недоліками даного методу є великий обсяг оброблювальної інформації, високий рівень кваліфікації експерта, великі затрати часу та матеріальних ресурсів.

Розроблений метод парето-оптимальних ФПЗ у [3, 8] базується на побудові підмножини, яка для кожної з величин видатків містить лише ті рішення, що дають найкращий рівень захищеності. Перехід від множини можливих рішень до аналізу лише однієї множини дозволяє наочно описати парето-оптимальні ФПЗ. У такий же спосіб для різних умов функціонування ІТС може бути сформоване ціле сімейство парето-оптимальних ФПЗ, серед яких у подальшому буде обрано як конкретну криву, так і конкретне парето-оптимальне рішення. Серед недоліків даного методу слід зазначити: високу кваліфікацію експерта; відхилення від нормативно-правової бази; багато часу на визначення профілів захищеності. Перевагою даного методу є можливість графічного визначення ФПЗ.

Авторами в роботі [5] було запропоновано теоретичні основи визначення стандартних ФПЗ автоматизованих систем від НСД. Даний метод ґрунтується на НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Його перевагами є автоматизація процесу визначення ФПЗ і середній рівень кваліфікації експерта.

Використання методів перевірки несуперечності та повноти профілю захищеності від НСД, побудови таксономії функціональних послуг безпеки, парето-оптимальних ФПЗ дає змогу оцінювати систему тільки щодо нестандартних профілів захисту, стандартні до

уваги не беруться, що призводить до невиконання стандартів з критеріїв оцінювання захисту системи. Кожний з розглянутих методів потребує великих затрат часу та матеріальних ресурсів для реалізації, що зумовлює їх нераціональне використання та потребує ґрунтовних знань у сфері ФПЗ.

З огляду на викладене вище можна сформулювати вимоги до методу визначення рівня захищеності ІТС:

зручність застосування;

зрозумілість проміжних результатів та їх вплив на остаточний склад ФПЗ;

врахування вимог НД;

коректність переходів між різними етапами визначення складу ФПЗ;

можливість самоперевірки;

наявність простого процесу вибору ФПЗ;

можливість визначення групової експертної оцінки.

Отже, актуальним є удосконалення методу формування стандартних ФПЗ, а саме створення програмного продукту їх автоматизованого визначення.

Висновки. Таким чином, у статті проаналізовано методи формування ФПЗ ІТС від НСД. Висвітлено необхідні НД ТЗІ, які регламентують порядок оцінювання. На їх базі вперше здійснено формалізацію основ визначення ФПЗ ІТС від НСД. З'ясовано, що розглянуті методи є складними в реалізації й вимагають в експерта ґрунтовних знань. Запропоновані авторами теоретичні основи в [5] та проведений аналіз методів дають можливість у подальшому розробити експертну систему, яка визначатиме ФПЗ ІТС від НСД. Це полегшить роботу експертів щодо визначення профілю захищеності та створення необхідного комплексу засобів захисту, а також зменшить необхідний ресурс часу.

СПИСОК ЛІТЕРАТУРИ

1. Лєншин А. В. Метод формування функціональних профілів захищеності від несанкціонованого доступу [Елекронний ресурс] / А. В. Лєншин, П. В. Буслов // Радіоелектронні і комп'ютерні системи : наук. журн. – Х. : ХАІ, 2010. – Т. 7. – С. 77–81. – Режим доступу : http://www.khai.edu/csp/nauchportal/Arhiv/REKS/2010/REKS710/Lyenshyn.pdf.

2. Паламарчук Н. А. Сучасний стан нормативно-правової бази в галузі технічного захисту інформації [Елекронний ресурс] / Н. А. Паламарчук, Ю. І. Хлапонін, В. В. Овсянніков // Зб. наук. 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.

3. 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.

4. 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.

5. 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.

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

7. Потій О. В. Методи побудови та верифікації несуперечності і повноти функціональних профілів захищеності від несанкціонованого доступу / О. В. Потій, А. В. Лєншин // Прикладная радиоэлектроника : науч. журнал. – Х. : ХАІ, 2010. – Т. 9, № 3. – С. 479–488.
8. Берестов Д. С. Метод пошуку проектних альтернатив системи захисту інформації / Д. С. Берестов, В. Л. Шевченко // Сучасний захист інформації. – К. : ДУТ, 2015. – № 3. – С. 22–27.
10. Yudin O. The analysis of normatively-legal providing of defence of state informative resources in information-telecommunication systems / O. Yudin, S. Buchyk // Science-based technologies. – 2013. – № 2 (18). – P. 202–206.

Подано 01.11.2017

Р. В. Нетребко

АНАЛИЗ НОРМАТИВНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ И МЕТОДОВ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В статье проанализировано нормативно-правовое обеспечение Украины и рассмотрены методы определения защищенности информационно-телекоммуникационной системы от несанкционированного доступа. Исследовано, с помощью каких нормативных документов оценивают уровень защищенности информационно-телекоммуникационных систем от несанкционированного доступа. В результате анализа установлен факт наличия малого количества нужных методов, проведено сравнение их между собой. Описаны преимущества и недостатки каждого с последующим формулированием требований по повышению эффективности определения функциональных профилей защищенности. Запланированы дальнейшие шаги исследования в определении уровня защищенности информационно-телекоммуникационной системы от несанкционированного доступа.

Ключевые слова: *нормативно-правовое обеспечение, уровень защищенности, информационно-телекоммуникационная система, несанкционированный доступ.*

R. V. Netrebko

ANALYSIS OF REGULATORY AND LEGAL SUPPORT AND METHODS FOR DETERMINING THE LEVEL OF SECURITY OF AN INFORMATION AND TELECOMMUNICATION SYSTEM FROM UNAUTHORIZED ACCESS

The article analyzes regulatory legal framework of Ukraine and methods of determining the security of the information-telecommunication system from unauthorized access. It was clarified with the help of which normative documents assess the level of protection of information-telecommunication systems from unauthorized access. As a result of the analysis, the fact of having a small number of required methods has been established and their number is reduced to five. A comparison is made between them. The advantages and disadvantages of each with the further formulation of requirements for increasing the effectiveness of defining functional security profiles are determined. Further research steps have been identified to assess the level of security of the information-telecommunication systems from unauthorized access.

Keywords: *regulatory legal framework, level of security, information-telecommunication system, unauthorized access.*