УДК 004.056.5

ТЕХНОЛОГІЯ ПОБУДОВИ ТА ЗАХИСТУ УКРАЇНСЬКОГО СЕГМЕНТА ДЕРЕВА ІДЕНТИФІКАТОРІВ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ РИЗИК-МЕНЕДЖМЕНТУ

Олександр Юдін, Сергій Бучик

У статті вперше представлена технологія побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів на основі ризик-менеджменту. Дана технологія базується на дослідженнях, які були проведені авторами раніше і пов'язана з вперше розробленою методологією побудови класифікатора загроз державним інформаційним ресурсам; проведеним аналізом світового дерева ідентифікаторів інформаційних ресурсів та місцем в ньому українського сегмента ідентифікаторів об'єктів; розробленою авторами структурно-логічною моделлю організації ієрархічної гілки кодів-вузлів українського сегмента ідентифікаторів об'єктів державних органів; розробленими моделями та принципами інформаційної безпеки, методами та моделями реалізації системи управління інформаційною безпекою державних інформаційних ресурсів; розробленими теоретичними основами та методологією аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів, іншими працями, що пов'язані єдиною метою – розробкою методології побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів. Впровадження даної технології повинно стати об'єднуючим фактором для узагальнення досвіду побудови захисту державних інформаційних ресурсів в країні на основі ризик-менеджменту та підходів, які не суперечать міжнародним стандартам.

Ключові слова: *технологія, державні інформаційні ресурси, дерево ідентифікаторів, ризик, ризик-менеджмент, рівень ризику, вузол інформаційно-телекомунікаційної системи.*

Актуальність дослідження. Для реалізації основних напрямів національної безпеки та протидії різним класам загроз інформаційним ресурсам, виникає необхідність розроблення науково обґрунтованої технології щодо побудови та захисту державних інформаційних ресурсів (ДІР) як складової національної безпеки держави. Виникає гостра потреба в необхідності володіти відповідним науково-методологічним апаратом побудови моделей політики безпеки, загроз, порушника, оцінки ризиків, вибору функціонального профілю захищеності та методів оцінки ефективності системи захисту ДІР. На теперішній час відсутня дієва технологія оцінки ризику ДІР, не класифіковані та не деталізовані їх загрози, відсутня система кодифікації ДІР та її адаптація до світових стандартів (в т.ч. до світового дерева ідентифікаторів). Тому *є актуальним*, з метою підвищення ефективності захисту ДІР в сучасних умовах інформаційного протиборства та зовнішньої агресії, необхідність створення дієвої технології побудови та захисту українського сегмента дерева ідентифікаторів ДІР на основі ризик-менеджменту.

Аналіз останніх досліджень та публікацій. Колектив авторів не один раз піднімав питання щодо необхідності впровадження в країні єдиної системи захисту ДІР. Нажаль така єдина система відсутня, тим більше технологія побудови та захисту українського сегмента дерева ідентифікаторів ДІР. Розробці даної технології передувала низка праць, пов'язаних єдиною метою, а саме розробкою методології побудови та захисту українського сегмента дерева ідентифікаторів ДІР. Таким чином, був розроблений класифікатор загроз ДІР нормативно-правового, організаційного та інженерно-технічного спрямування на основі методу «подвійної трійки захисту» [1], що дозволило визначити функціональні профілі (ФП) загроз. Розроблено метод оцінки функціональних профілів загроз [2] з урахуванням вимог міжнародного стандарту інформаційної безпеки серії ISO/IEC 2700x, який до сих пір в Україні не введено на рівні ДСТУ, хоча в окремих державних і недержавних галузях він використовується (наприклад Національним банком України ведені «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України» [3]. Відповідно з Постановою Національного банку України від 28.10.2010 р. №474 набрали чинності такі стандарти Національного банку України: СОУ Н НБУ 65.1 СУІБ 1.0:2010 "Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги" (ISO/IES 27001 : 2005, MOD); СОУ Н НБУ 65.1 СУІБ 2.0 : 2010 "Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою" (ISO/IES

27002 : 2005, MOD) [4]). В подальшому автором були розроблені теоретичні основи [5] та методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів [6], здійснено формалізацію визначення стандартних профілів захищеності автоматизованої системи від несанкціонованого доступу [7]. Безпосередньо підхід до узагальнення всього вищевикладеного авторами представлено в загальній моделі формування системи захисту ДІР [8].

В зв'язку з тим, що основа представленої нижче технології пов'язана з ризик-менеджментом, є доречним здійснити аналіз праць, які присвячені питанню управління інформаційними ризиками.

У цілому питанню управління інформаційними ризиками присвячено наукові праці, у яких наведено значну кількість формул, різного роду принципів, визначено кількісні та якісні підходи, використано теорію корисності, суб'єктивної ймовірності, безперервні розподілення, теорію нечітких множин та інше. Питанням оцінки факторів ризику інформаційної безпеки присвячено роботи Корченка О. Г. [9], основою якої є теорія нечітких множин, Астахова А. М. [10], який використовує системний підхід до управління інформаційними ризиками, що ґрунтується на міжнародних стандартах BS 7799–3 та ISO 27005, Гончара С. Ф [11], де використано ймовірнісний підхід, Дмітриєва О. А. [12], що розкриває питання ризик-менеджменту відповідно до міжнародних стандартів ISO/IEC 27001, Чернея Г. А. [13], у якій поєднаний експертний та ймовірнісний підхід до аналізу інформаційних ризиків. В роботі [14] здійснено спробу узагальнити всі основні моделі менеджменту інформаційної системи щодо безпеки ризиків. В роботі [15] здійснено спробу аналізу менеджменту ризику ІБ в телекомунікаційних мережах. В [16] розкриті алгебраїчні специфікації ризик-менеджменту безпеки мереж на основі побудови сигнатур ризиків, використання логіки предикатів та вейвлет перетворень.

Таким чином, на думку авторів, важливим при розробці технології побудови та захисту українського сегмента дерева ідентифікаторів ДІР на основі ризик-менеджменту є використання найбільш простого та доступного апарату, який матиме властивість практичної корисності та поєднуватиме в собі кращі сторони решти підходів та не вступає у протиріччя з міжнародними стандартам.

Мета статті. Метою статті є розробка технології побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів на основі ризик-менеджменту.

Виклад основного матеріалу. Виходячи з наведеного аналізу та мети статті, необхідно на базі розробленої методології побудови класифікатора загроз ДІР представленої в [1, 17], українського сегменту ідентифікаторів об'єктів, представленого у [1], моделей та принципів інформаційної безпеки (ІБ) ДІР, методів та моделей реалізації системи управління інформаційною безпекою (СУІБ) ДІР розкритих у [8, 18, 19], розроблених теоретичних основ [5] та методології аналізу ризиків дерева ідентифікаторів ДІР [6], представити технологію побудови та захисту дерева ідентифікаторів ДІР на основі ризик-менеджменту.

Технологія побудови та захисту українського сегменту дерева ідентифікаторів ДІР на основі ризик-менеджменту полягає у наступному (рис. 1):

1. Вибір функціональних профілів загроз для обраного вузла інформаційно-телекомунікаційної системи (ІТС) українського сегмента дерева ідентифікаторів ДІР із класифікатора загроз, методологія побудови якого, та приклади класифікації загроз нормативно-правового (НПС), організаційного (ОргС) і інженерно-технічного спрямування приведена (ІнжТС) в [1, 17].

2. Здійснення оцінювання функціональних профілів загроз та отримання комплексної оцінки по кожному профілю за методикою, визначеною в [2].

3. За визначеними критеріями прийнятності відбір необхідних функціональних профілів загроз (порядок визначення приведено в [2]).

4. На основі відібраних функціональних профілів загроз здійснити розрахунок ризиків вузла ІТС українського сегмента дерева ідентифікаторів ДІР за допомогою методів, розроблених в [5, 6].

5. За п.1–4 технології здійснити розрахунок ризиків всіх вузлів ІТС українського сегмента дерева ідентифікаторів ДІР.

6. На основі транзитивного замикання бінарного відношення побудувати дерево вузлів ІТС українського сегмента ідентифікаторів державних інформаційних ресурсів з урахуванням їх групування за α – рівнями та визначення оптимальної топології з'єднання вузлів з урахуванням їх ризиків.

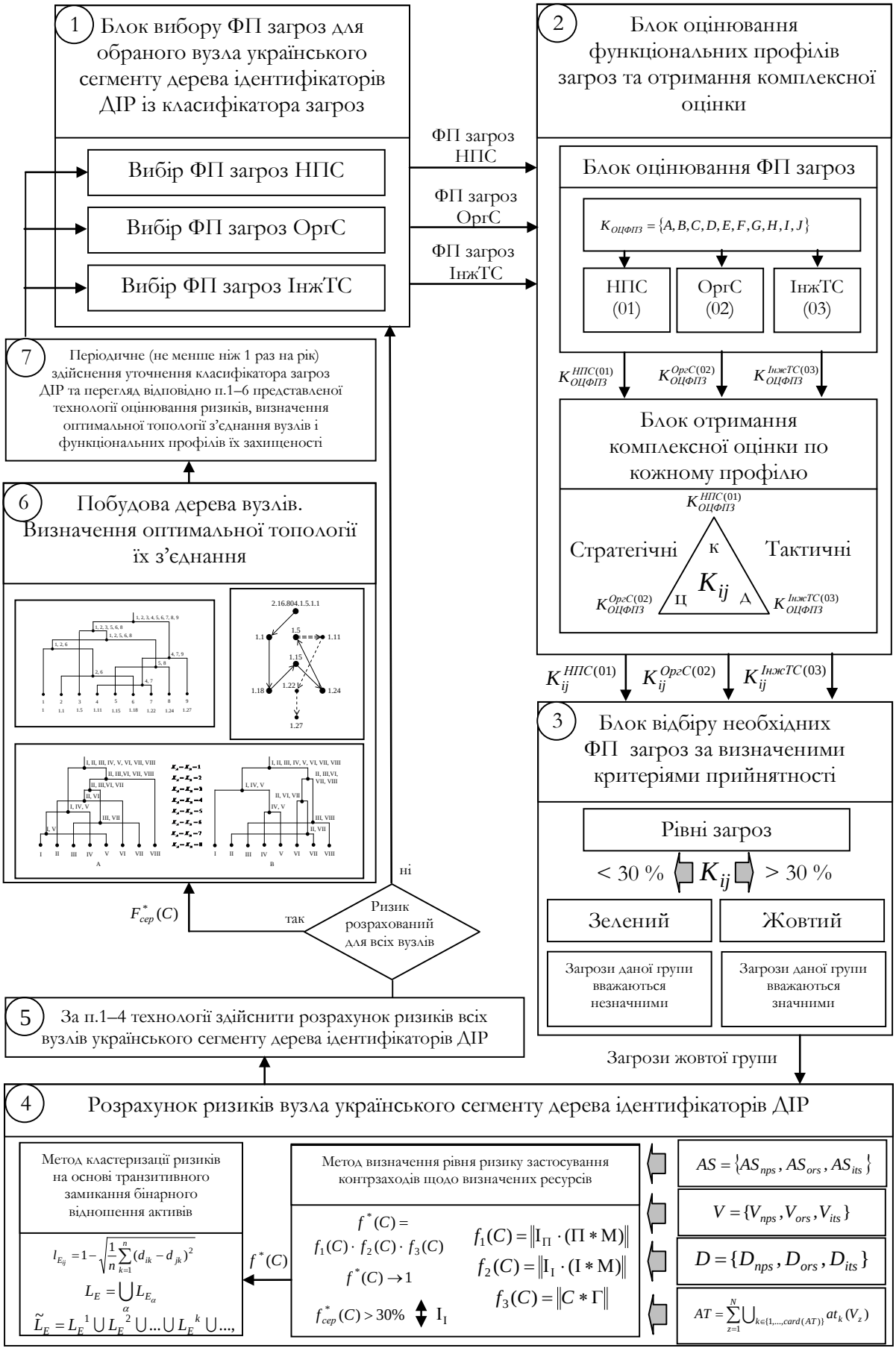


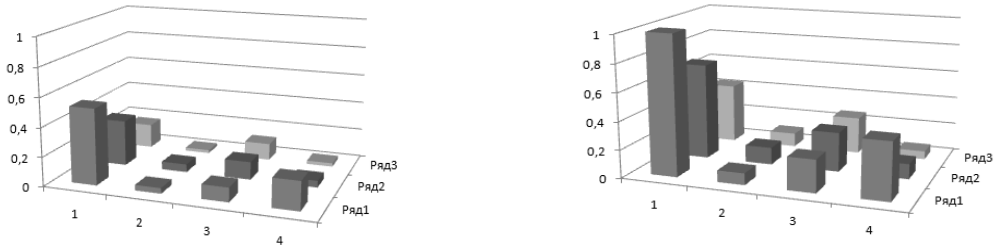
Рис. 1. Технологія побудови та захисту українського сегменту дерева ідентифікаторів ДІР на основі ризик-менеджменту

7. Періодичне (не менше ніж 1 раз на рік) здійснення уточнення класифікатора загроз ДІР та перегляд відповідно п.1–6 представленої технології оцінювання ризиків, визначення оптимальної топології з'єднання вузлів ІТС і функціональних профілів їх захищеності.

Підхід даної технології відповідає так званому процедурному підходу та використанню моделі «Plan-Do-Check-Act» (PDCA – цикл Шухарта-Деминга – планування – реалізація – перевірка – дія), який розкритий у міжнародному стандарті серії ISO/IEC 27001 [20].

Обмеженням при реалізації даної технології є відсутність врахування пропускної здатності ліній передачі інформації між вузлами ІТС, що може бути в подальшому реалізовано шляхом введення ваги, яка б визначала пропускну здатність відповідної лінії.

За визначеною технологією було здійснено розрахунок ризику використання ІТС вузла 2.16.804.1.5.1.1.11 (розкриття організації ієрархічної гілки кодів-вузлів українського сегмента ідентифікаторів об'єктів державних органів представлено в [1]) на основі відібраних за критерієм прийнятності ФП загроз. На рис. 2a представлено ступінь забезпечення захисту ресурсів до оптимізації та на рис. 2b після проведення оптимізації.



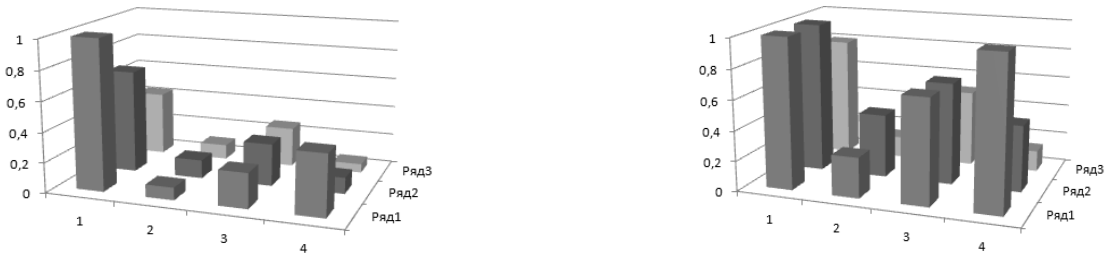
a) b)

Рис. 2. Ступінь забезпечення захисту ресурсів до оптимізації (a) та після оптимізації (b)

Середнє значення ризику, яке буде характеризувати ризик всієї ІТС вузла ідентифікатора об'єктів, склало $C^*_{сер} = 0{,}3145$. Таким чином, середній ризик даного вузла ІТС буде складати 68,55 %. Даний рівень є дуже великим і неприпустимим.

Для зменшення ризику необхідно здійснити регулювання матриці I_I, яка відповідає впливу прийнятого рішення d_i на ймовірність атаки at_k, тобто необхідно налаштувати засоби захисту таким чином, щоб вплив прийнятого рішення d_i на ймовірність атаки at_k був не нижче прийнятного рівня (в нашому випадку не вище 30%, виходячи з критерію обрання функціональних профілів загроз).

Після проведення регулювання матриці I_I здійснимо повторне оцінювання ризику визначеного вузла ІТС. Для наочності знов порівняємо ступінь забезпечення захисту ресурсів після оптимізації (рис. 3a), який повторює рис. 2b та з урахуванням регулювання матриці I_I.



a) b)

Рис. 3. Ступінь забезпечення захисту ресурсів до оптимізації (a) та після оптимізації (b) з урахуванням регулювання матриці I_I.

Порівнюючи рис. 3a з 3b вже наочно можна прослідкувати збільшення ступеня захисту ресурсів.

Середнє значення ризику, яке буде характеризувати ризик всієї ІТС вузла ідентифікатора об'єктів, склало $C^*_{сер} = 0{,}591$. Таким чином, середній ризик даного вузла ІТС з урахуванням регулювання матриці I_I буде складати 40,922 %, що в 1,67 рази менший ніж попередній.

Для визначення ефективності даного методу оцінювання та подальшого регулювання ризиків було проведено імітаційне моделювання шляхом генерування за нормальним розподілом псевдовипадкових величин для формування вихідних матриць. Результати моделювання показали, що середній ризик з урахуванням регулювання матриці I_1 може бути зменшений в 1,5 – 2 рази.

Основні результати. До основних результатів досліджень, викладених у статті, можна віднести вперше розроблену технологію побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів на основі ризик-менеджменту, що дозволило здійснювати корегування та оптимізацію засобів захисту (необхідних контрзаходів) визначених інформаційних активів (ресурсів) та здійснювати зменшення середнього рівня ризику вузла інформаційно-телекомунікаційної системи в 1,5 – 2 рази. Результат використання транзитивного замикання бінарного відношення середніх рівнів ризику вузлів інформаційно-телекомунікаційної системи та визначення оптимального α – рівня (алгоритм визначення представлено в [21]) дозволяє отримати оптимальний шлях передачі повідомлень між вузлами ієрархічного дерева ідентифікаторів об'єктів та розбити цей шлях на кластери за рівнями ризику, що дозволяє до 50 % зменшити ризик несанкціонованого доступу до повідомлень, які передаються між вузлами інформаційно-телекомунікаційної системи.

Висновок. В результаті проведених досліджень автором представлено вперше розроблену технологію побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів на основі ризик-менеджменту, яка містить в собі елементи розробленої загальної моделі формування системи захисту ДІР, що дозволило знизити інформаційний ризик вузла ідентифікатора об'єкту та визначити ефективність контрзаходів, які використовуються. Впровадження розроблених методів аналізу ризиків дерева ідентифікаторів ДІР дозволило здійснювати корегування та оптимізацію засобів захисту (необхідних контрмір) щодо визначених активів (ресурсів) та наочно відслідковувати процес групування активів у кластери для їх подальшого аналізу, що дало змогу в 1,5 – 2 рази знизити інформаційний ризик вузла ідентифікатора об'єктів та до 50 % зменшити ризик несанкціонованого доступу до повідомлень, які передаються між вузлами інформаційно-телекомунікаційної системи.

ЛІТЕРАТУРА

[1]. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик – К. : НАУ, 2015. – 214 с.

[2]. Бучик С.С. Оцінка функціональних профілів загроз державним інформаційним ресурсам / С. С. Бучик // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. – Житомир: ЖВІ ДУТ, 2014. – Вип. 9. – С. 146 – 155.

[3]. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України : лист Департаменту інформатизації Національного банку України від 03.03.2011 №24-112/365 банкам України [Електронний ресурс]. – Режим доступу: http: // zakon5. rada.gov.ua/laws/show/v0365500-11.

[4]. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України : Постанова Правління Національного банку України від 28.10.2010 №474 [Електронний ресурс]. – Режим доступу: http: // zakon5. rada. gov. ua/laws/show/v0474500-10

[5]. Бучик С. С. Теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С. С. Бучик // Наукоємні технології. – 2016. – № 1 (29). – С. 70 – 77.

[6]. Бучик С. С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С. С. Бучик // Захист інформації. – 2016 – №1 (18). – С. 81 – 89.

[7]. Бучик С.С. Формалізація визначення стандартних профілів захищеності автоматизованої системи від несанкціонованого доступу / Бучик С.С., Мельник С. В. // Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення з урахуванням досвіду антитерористичної операції : XXI Всеукр. наук.-практ. конф., 21 квітня 2016 р. : тези доповідей. – Житомир : ЖВІ, 2016. – С. 127 – 129.

[8]. 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.

[9]. Корченко А. Г. Построение систем защиты информации на нечётких множествах. Теория и практика решения / А. Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

[10]. Астахов А. М. Искусство управления информационными рисками / А. М. Астахов. – М. : ДМК Пресс, 2010. – 312 с.

[11]. Гончар С. Ф. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом / С. Ф. Гончар // Захист інформації. – 2014. – № 1(16). – С. 40 – 46.

[12]. Дмитриев А. А. Риск-менеджмент по требованиям международного стандарта ISO/IEC 27001. Один из способов увидеть будущее без машины времени [Электронный ресурс] / А. А. Дмитриев. – Режим доступа: http://www.das-management.info.

[13]. Черней Г. А. Оценка угроз безопасности автоматизированным информационным системам [Электронный ресурс] / Г. А. Черней. – Режим доступа: http://www.ase.md/~osa/publ/ru/pubru01.html

[14]. N. Mayer, "Model-Based Management of Information System Security Risk", Namur, Belgium, 2009, ISBN : 978-2-87037-640-9.

[15]. Jihene Krichene. Managing Security Projects in Telecommunication Networks : To obtain Diploma of Doctor in Information and Communications Technology / Krichene Jihene. – Tunis: 2008. – 204 p.

[16]. M. Hamdi, X. Boudriga, "Algebraic Specification of Network Security Risk Management'" First ACM Workshop on Formal Methods in Security Engineering, Washington D.C., 2003.

[17]. Юдін О. К. Методологія побудови класифікатора загроз державним інформаційним ресурсам / О. К. Юдін, С. С. Бучик, А. В. Чунарьова, О. І. Варченко // Наукоємні технології. – 2014. – № 2 (22). – С. 200 – 210.

[18]. Юдін О. К. Концептуальна модель інформаційної безпеки державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. – 2014. – № 4 (24). – С. 462 – 466.

[19]. Юдін О. К. Принципи побудови комплексної системи захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. – 2015. – № 1 (25). – С. 15 – 20.

[20]. Information Security Management – Specification With Guidance for Use: ISO/IEC 27001 : 2013 [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/catalogue_detail? Csnumber =54534.

[21]. Герасимов Б. М. Алгоритм визначення α - рівня нечіткого відношення / Б. М. Герасимов, С. С. Бучик, О. С. Кондратенко // Збірник наукових праць ВІТІ НТУ України "КПІ". – К.: ВІТІ НТУУ "КПІ", 2005. – Вип. 3. – С. 8 – 12.

REFERENCES

[1]. Yudin O., Buchyk S. Derzhavni informatsiyni resursi. Metodologiya pobudovi klasifikatora zagroz : monografiya, K: NAU, 2015, 214 p.

[2]. Buchik S.S. (2015) "Otsinka funktsionalnih profiliv zagroz derzhavnim informatsiynim resursam", Problemi stvorennya, viprobuvannya, zastosuvannya ta ekspluatatsiyi skladnih informatsiynih sistem : zb. nauk. prats, Zhitomir: ZhVI DUT, Vip. 9, pp. 146-155.

[3]. Metodychni rekomendatsiyi shchodo vprovadzhennya systemy upravlinnya informatsiynoyu bezpekoyu ta metodyky otsinky ryzykiv vidpovidno do standartiv Natsional'noho banku Ukrayiny : lyst Departamentu informatyzatsiyi Natsional'noho banku Ukrayiny vid 03.03.2011 №24-112/365 bankam Ukrayiny [Elektronnyy resurs]. – Rezhym dostupu: http: // zakon5.rada.gov.ua/laws/show/v0365500-11.

[4]. Pro nabrannya chynnosti standartamy z upravlinnya informatsiynoyu bezpekoyu v bankivs'kiy systemi Ukrayiny : Postanova Pravlinnya Natsional'noho banku Ukrayiny vid 28.10.2010 №474 [Elektronnyy resurs]. – Rezhym dostupu: http://zakon5.rada.gov.ua/laws/show/v0474500-10.

[5]. Buchik S.S. (2016) " Teoretychni osnovy analizu ryzykiv dereva identyfikatoriv derzhavnykh informatsiynykh resursiv ", Science-based technologies, №1 (29), pp. 70 – 77.

[6]. Buchik S.S. (2016) "Metodolohiya analizu ryzykiv dereva identyfikatoriv derzhavnykh informatsiynykh resursiv", Ukrainian Information Security Research Journal, №1 (18), pp. 81 – 89.

[7]. Buchik S.S., Melnyk S. V. (2016) "Formalizatsiya vyznachennya standartnykh profiliv zakhyshchenosti avtomatyzovanoyi systemy vid nesanktsionovanoho dostupu", Problemy stvorennya, rozvytku ta zastosuvannya vysokotekhnolohichnykh system spetsial'noho pryznachennya z urakhuvannyam dosvidu antyteroorystychnoyi operatsiyi : XXI Vseukr. nauk.-prakt. konf., 21 kvitnya 2016 r. : tezy dopovidey, Zhitomir: ZhVI. – pp. 127 – 129.

[8]. Yudin O., Buchyk S., Frolov O. (2015) "Zagalna model formuvannya sistemi zahistu derzhavnih informatsiynih resursiv", Science-based technologies, №4(28), pp. 332 – 337.

[9]. Korchenko O. Postroenye system zashchytu informatsii na nechëtkykh mnozhestvakh. Teoryya y praktyka reshenyya, K: MK-Press, 2006, 320 p.

[10].Astahov A. M. Iskusstvo upravleniya informatsionnyimi riskami, M.: DMK Press, 2010, 312 p.

[11]. Honchar S. (2014) "Analiz ymovirnosti realizatsiyi zahroz zakhystu informatsiyi v avtomatyzovanykh systemakh upravlinnya tekhnolohichnym protsesom", Ukrainian Information Security Research Journal, № 1 (16), pp. 40 – 46.

[12]. Dmitriyev A. "Risk-menedzhment po trebovaniyam mezhdunarodnogo standarta ISO/IEC 27001. Odin iz sposobov uvidet budushcheye bez mashiny vremeni" [Elektronnyy resurs]. – Rezhim dostupa: http://www.das-management.info.

[13]. Cherney G. "Otsenka ugroz bezopasnosti avtomatizirovannym informatsionnym sistemam" [Elektronnyy resurs]. – Rezhim dostupa: http:// www.ase.md/~osa/publ/ru/pubru01.html.

[14]. N. Mayer, "Model-Based Management of Information System Security Risk", Namur, Belgium, 2009, ISBN : 978-2-87037-640-9.

[15]. Jihene Krichene. Managing Security Projects in Telecommunication Networks : To obtain Diploma of Doctor in Information and Communications Technology / Krichene Jihene. – Tunis: 2008. – 204 p.

[16]. M. Hamdi, X. Boudriga, "Algebraic Specification of Network Security Risk Management'" First ACM

Workshop on Formal Methods in Security Engineering, Washington D.C., 2003.
[17]. Yudin O., Buchyk S., Chunareva A., Frolov O. (2014) "Methodology of construction of classifier of threats to the state informative resources", Science-based technologies, №2 (22), pp.200 – 210.
[18]. Yudin O., Buchyk S. "Kontseptual'na model' informatsiynoyi bezpeky derzhavnykh informatsiynykh resursiv", Science-based technologies, №4 (24), pp. 462 – 466.
[19]. Yudin O., Buchyk S. (2015) "Pryntsypy pobudovy kompleksnoyi systemy zakhystu derzhavnykh informatsiynykh resursiv", Science-based technologies, № 1 (25), pp. 15 – 20.
[20]. Information Security Management – Specification With Guidance for Use: ISO/IEC 27001 : 2013 [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=54534.
[21]. Gerasimov B., Buchik S., Kondratenko S. (2005) "Algoritm viznachennya α - rivnya nechitkogo vidnoshennya", Zbirnik naukovih prats VITI NTU Ukraine "KPI", K.: VITI NTUU "KPI", Vip. 3, pp. 8-12.

ТЕХНОЛОГИЯ ПОСТРОЕНИЯ И ЗАЩИТЫ УКРАИНСКОГО СЕГМЕНТА ДЕРЕВА ИДЕНТИФИКАТОРОВ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ НА ОСНОВЕ РИСК-МЕНЕДЖМЕНТА

В статье впервые представлена технология построения и защиты украинского сегмента дерева идентификаторов государственных информационных ресурсов на основе риск-менеджмента. Данная технология базируется на исследованиях, которые были проведены авторами раньше и связана с впервые разработанной методологией построения классификатора угроз государственным информационным ресурсам; проведенным анализом мирового дерева идентификаторов информационных ресурсов и местом в нем украинского сегмента идентификаторов объектов; разработанной авторами структурно-логической моделью организации иерархической ветки кодов-узлов украинского сегмента идентификаторов объектов государственных органов; разработанными моделями и принципами информационной безопасности, методами и моделями реализации системы управления информационной безопасностью государственных информационных ресурсов; разработанными теоретическими основами и методологиею анализа рисков дерева идентификаторов государственных информационных ресурсов, других трудов, которые связаны единой целью – разработкою методологии построения и защиты украинского сегмента дерева идентификаторов государственных информационных ресурсов. Внедрение данной технологии должно стать объединительным фактором для обобщения опыта построения защиты государственных информационных ресурсов в стране на основе риск-менеджмента и подходов, которые не противоречат международным стандартам.

Ключевые слова: технология, государственные информационные ресурсы, дерево идентификаторов, риск, риск-менеджмент, уровень риска, узел информационно-телекоммуникационной системы.

TECHNOLOGY OF CONSTRUCTION AND DEFENCE OF THE UKRAINIAN SEGMENT OF THE IDENTIFIERS' TREE OF STATE INFORMATIVE RESOURCES ON THE BASIS OF RISK MANAGEMENT

In the article a technology of construction and defence of the Ukrainian segment of the tree of identifiers of state informative resources on the basis of risk management is presented for the first time. This technology is based on researches that were conducted by the authors before and are related to the first worked out methodology of construction of a classifier of threats to the state informative resources; to the conducted analysis of the world tree of identifiers of informative resources and to the place of the Ukrainian segment of identifiers of objects in it; to the structural-logical model of organization of hierarchical branch of codes-knots of the Ukrainian segment of identifiers of objects of public organs; to models and principles of informative safety worked out by the authors, methods and models of realization of control system of informative safety of the state informative resources; to worked out theoretical bases and methodology of analysis of risks of the tree of identifiers of state informative resources, to other works that are bound by the only aim - the development of the methodology of construction and defence of the Ukrainian segment of the tree of identifiers of the state informative resources. Introduction of this technology must become a unifying factor for generalization of experience of construction of defence of the state informative resources in the country on the basis of risk management and approaches that do not conflict with international standards.

Keywords: technology, state informative resources, tree of identifiers, risk, risk-management, risk level, knot of the information-telecommunication system.

Юдін Олександр Костянтинович, доктор технічних наук, професор. Член експертної та науково-методичної ради Міністерства освіти та науки України в галузі "Інформаційна безпека". Член-кореспондент Академії Зв'язку України. Лауреат Державної премії України у галузі науки і техніки. Директор навчально-наукового інституту комп'ютерних інформаційних технологій Національного авіаційного університету.
E-mail: kszi@ukr.net
Юдин Александр Константинович, доктор технических наук, профессор. Член экспертного и научно-методического совета Министерства образования и науки Украины в области "Информационная безопасность".

Член-корреспондент Академии Связи Украины. Лауреат Государственной премии Украины в области науки и техники. Директор учебно-научного института компьютерных информационных технологий Национального авиационного университета.

Yudin Alexander, D. of Engineering, professor. Member of expert and scientifically-methodical advice of Department of education and science of Ukraine in an area "Informative security". Corresponding member of Academy of Connection of Ukraine. Laureate of the State bonus of Ukraine in area of SciTech. Director of Education and Research institute of computer information technologies the National Aviation University.

Бучик Сергій Степанович, кандидат технічних наук, доцент, начальник кафедри автоматизованих систем управління Житомирського військового інституту імені С. П. Корольова.
E-mail: s_stbu@ukr.net

Бучик Сергей Степанович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления Житомирского военного института имени С.П. Королева.

Buchyk Sergii, PhD in Eng., chief of department of automated control the system the Zhitomir Military Institute of the name of S.P. Korolyova.

УДК 511.512

АЛГОРИТМ БАЙТ–ОРИЕНТИРОВАННОГО ПОТОЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ РАВНОМЕРНО ПЛОТНЫХ БЛОКОВ НЕЛИНЕЙНОЙ ПОДСТАНОВКИ

Анатолий Белецкий, Денис Навроцкий, Александр Семенюк

В статье рассматриваются вопросы построения нового байт-ориентированного алгоритма синхронного поточного шифрования, в котором шифрующая гамма-последовательность стохастических битов формируется совокупностью равномерно плотных примитивов нелинейной подстановки (S-блоков). Равномерно плотными являются такие примитивы нелинейной подстановки, отклики которых равномерно распределены на поверхности диаграммы рассеяния примитива. Предложен вариант синтеза равномерно плотных S-блоков, диаграммы рассеяния которых превышают качественные характеристики соответствующих показателей диаграммы рассеяния блока нелинейной подстановки алгоритма Rijndael. Проведен сравнительный анализ эффективности разработанного криптопреобразования и наиболее популярного AES-алгоритма в режиме поточного шифрования. Обсуждаются направления применения предлагаемых шифров в различных приложениях.

Ключевые слова: *алгоритмы синхронного поточного шифрования, равномерно плотные блоки нелинейной подстановки, криптографическая защита информации.*

1. Введение и постановка задачи. Различают два основных класса алгоритмов шифрования: блочные и поточные. В *блочных шифрах* в результате криптопреобразования двух одинаковых блоков открытого текста образуются два одинаковых блока шифрованного текста. Избежать этого позволяют *поточные шифры* [1-2], в которых шифрующее преобразование «элемента» открытого текста меняется от одного элемента к другому. Такой эффект прослеживается, например, в блочных DES и AES шифрах, которые в режиме сцепления блоков фактически преобразуются в поточные шифры.

На практике термин поточный шифр используют, как правило, только в том случае, когда «элементы» открытого текста очень малы и составляют один бит или один байт. Если шифруемым элементом является бит, то такие поточные шифры называют *бит-ориентированными шифрами* [3]. Если же шифруемым элементом служит байт, то шифры называют *байт-ориентированными* [4]. Реже встречаются поточные шифры, размер шифруемых элементов в которых превышает байт [5].

Большинство поточных шифров могут быть названы *двоичными аддитивными шифрами* [6]. В таких шифрах $k-$битный секретный ключ K используется только для управления генератором, порождающего *псевдослучайную последовательность* (ПСП) битов $k_0, k_1, \ldots, k_{N-1}$, называемую *ключевым потоком* $\mathcal{K}$, где $N >> k$. Шифртекст C образуется путем сложения по модулю 2 битов T_i открытого текста T и битов k_i ключевого потока $\mathcal{K}$, в результате чего приходим к алгоритму шифрования

$$C_i = T_i \oplus k_i, \qquad i = 0,1,\ldots,N-1.$$

Дешифрование криптограммы C выполняется аналогично алгоритму шифрования открытого текста T, т. е. $T_i = C_i \oplus k_i$.

Поточные шифры находят применение в тех случаях, когда требуется высокая скорость передачи информации, например, при трансляции «живого» видео, в системах сотовой связи и др.,