resurs] / Iryna Tytarchuk. — Kyiv: Agravery.com. — 2020. Rezhym dostupu do resursu: https://cutt.ly/ptvFASy [in Ukrainian]

Стаття надійшла до редакції 25.03.2020 р.

УДК 339.9
JEL Classification M15
DOI 10.33111/EE.2020.44.MakovskyiI

I. Makovskyi
PhD-student, Department of Management and Entrepreneurship, State University «Zhytomyr Polytechnic»

І. Ю. Маковський
аспірант кафедри менеджменту і підприємництва, Державний університет «Житомирська політехніка»

ORCID: https://orcid.org/0000-0002-9902-0364

КРИТЕРІАЛЬНИЙ АНАЛІЗ ПРОФІЛЮ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

АНОТАЦІЯ. У статті проведено аналіз критеріїв оцінки захищеності інформації, що циркулює в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах підприємства. Такий аналіз спрямований на визначення та формування мінімально-необхідного й достатнього функціонального профілю захищеності інформації на конкретному підприємстві в цілому, а також у процесі реалізації окремих бізнес-процесів. При цьому особливу увагу зосереджено на рентабельності реалізації обраного профілю захищеності, тобто, на співвідношенні збитків, що їх може завдати витік/втрата тієї чи іншої інформації до видатків, необхідних для реалізації відповідного профілю захищеності інформації. Окрім того, закладено підґрунтя для подальших досліджень щодо формування політики інформаційної безпеки на підприємстві з урахуванням рентабельності впровадження тих чи інших заходів.
КЛЮЧОВІ СЛОВА: критерії захищеності, конфіденційність, цілісність, доступність, спостережність, критерії гарантій, профіль захищеності.

CRITERIONAL ANALYSIS OF THE PROFILE OF INFORMATION SECURITY AT THE ENTERPRISE

ANNOTATION. The article analyzes the criteria for assessing the security of information circulating in information, telecommunication and information and telecommunication systems of the enterprise.

Such analysis is aimed at identifying and forming a minimum-necessary and sufficient functional profile of information security at a particular enterprise as a whole, as well as in the process of implementing individual business processes. Special attention is paid to the profitability of implementing the selected security profile, that is, to the ratio of losses that can be caused by the leakage / loss of a particular information to the expenses necessary for the implementation of the respective security profile. The article analyzes in detail the criteria of confidentiality, integrity criteria, accessibility criteria and criteria for the observation of information that circulates in information and telecommunication systems, as well as requirements for architecture, development environment, design process, environment, documentation and testing of the complex of facilities, that make up the warranty criterion. Particular attention is paid to the fact that the implementation of some security services is a prerequisite for the implementation of other services, so there are services without which it is impossible to implement a system of access delimitation, to implement functions that require the appointment of a system administrator, in particular administrative delimitation of access and to implement the service of integrity of the complex of means protection, which is also mandatory. In addition laid the groundwork for further research on the formation of information security policy at the enterprise, taking into account the profitability of implementing certain measures.
KEY WORDS: security criteria, privacy, integrity, availability, observance, warranty criteria, security profile.

Вступ. Стаття має на меті проведення аналізу критеріїв оцінки захищеності інформації, що циркулює в інформаційно-телекомунікаційних системах підприємства. Такий аналіз дозволить у подальшому сформувати оптимальний функціональний профіль захищеності інформації, що задовольнить потребу підприємства в захисті критичних даних за мінімальних витрат на його реалізацію.

Постановка завдання. Виходячи з результатів попередніх досліджень, в яких було проаналізовано вихідні дані, необхідні для формування політики інформаційної безпеки підприємства, а саме загрози інформації та їх потенційні носії (порушники безпеки) [1], постає потреба проаналізувати критерії оцінки захищеності інформації в інформаційно-телекомунікаційних системах підприємствах. Такий аналіз необхідний для формування функціонального профілю захищеності інформації, що задовольняв би потреби політики інформаційної безпеки за мінімальних видатків на реалізацію профілю захищеності.

Проблему відсутності чітких критеріїв захищеності інформації та визначення рівнів захищеності для різних видів загроз у своїх працях розглядали Н.П. Бортник, С.В. Пєтков [2], Я.І. Заячук [3], М.Г. Романюков [4] та інші.

Результати. Чинна нормативно-правова база пропонує можливий набір критеріїв захищеності, на підставі яких формується функціональний профіль захищеності інформації на кожному конкретному підприємстві чи в організації [5]. Такий профіль складається на підставі аналізу загроз і ймовірних порушників, виходячи з потреб і пріоритетів підприємства в захисті відповідних інформаційних ресурсів. Стандартні профілі захищеності подані в нормативному документі системи технічного захисту інформації НД ТЗІ 2.5-005-99 [6].

Отже розглянемо критерії захищеності інформації. Відповідно до нормативних документів критерії оцінювання утворюють систему з п'яти груп або категорій:

- критерії конфіденційності;
- критерії цілісності;
- критерії доступності;
- критерії спостережності;
- критерії гарантій.

Критерії з перших чотирьох груп є функціональними, тобто, визначають, які послуги безпеки здатна надавати система, що підлягає оцінці захищеності. До надання кожної з послуг безпеки висувається низка відповідних вимог, за якими визначається рівень надання такої послуги. Множина рівнів послуг безпеки, що їх надає система, складає функціональний профіль захищеності. Критерії гарантії визначають рівень правильності й відповідності реалізації послуг безпеки.

Вимоги до послуг безпеки згруповано за ознакою кінцевої мети їх реалізації, тобто, захисту окремої властивості інформації або системи. Така систематизація зручна для кінцевого споживача захищеної системи, оскільки спрямована саме на задоволення його потреб у захисті інформації.

Перш ніж переходити до розгляду кожного з конкретних критеріїв захищеності, слід усвідомити, що, по-перше, жоден з критеріїв неможливо визначити окремо один від одного й, по-друге, потрібно враховувати, що чим вищий рівень захищеності хоче бачити власник інформації, то дорожчою буде його реалізація. Кажучи про зростання вартості забезпечення безпеки інформації, ми вбачаємо не лише видатки на закупівлю обладнання чи програмного забезпечення, враховувати слід також потребу в оплаті праці додаткового персоналу, а також залучених зовнішніх спеціалістів.

З метою формування потрібного функціонального профілю захищеності фахівець з інформаційної безпеки разом з керівни-

ком підприємства повинен, зваживши загрози, визначити заходи, що відповідали б мінімально необхідним критеріям захищеності.

Отже розглянемо, що означає кожен з критеріїв, які пропонують чинні українські нормативні акти. Почнемо з критеріїв конфіденційності (рис. 1).

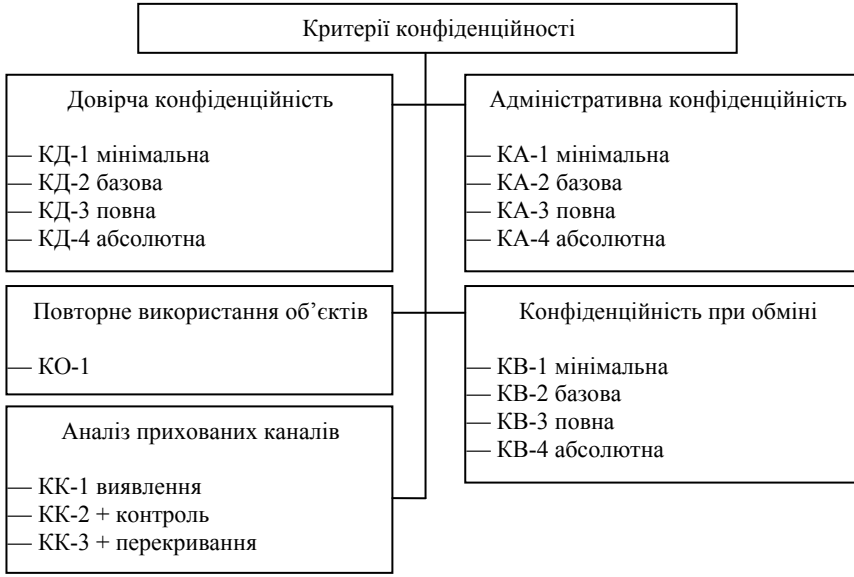

Рис. 1. Критерії конфіденційності

Перелічені критерії дозволяють оцінити, наскільки спроможна створена система захисту інформації надавати послуги із захисту об'єктів від несанкціонованого ознайомлення з їх змістом, тобто, здатність системи інформаційної безпеки захистити конфіденційну інформацію від компрометації. Як видно з рисунка, до складу послуг безпеки, що забезпечують конфіденційність, входять: довірча й адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність під час обміну.

Будь-яка система керування доступом надає дві послуги, що безпосередньо забезпечують реалізацію розмежування доступу активних об’єктів до пасивних об’єктів. Довірча конфіденційність передбачає надання дозволу активним об’єктам (користувачам чи процесам) самостійно скеровувати інформаційні потоки від захищених елементів системи, що належать їхньому домену,

до інших користувачів чи споживачів інформації. За допомогою послуги адміністративної конфіденційності вже адміністратор або спеціально авторизований користувач може спрямовувати інформаційні потоки від захищених об'єктів до користувачів. Кожна з цих двох послуг має чотири рівні, що базуються на повноті захисту й вибірковості керування. При цьому мінімальний (КД-1 та КА-1 відповідно) і базовий (КД-2 та КА-2) рівні передбачають, що дія послуги поширюється на певну множину об’єктів системи, а повний (КД-3 та КА-3) й абсолютний рівні — на всі об'єкти доступу в системі. Мінімальний рівень вимагає контролю атрибутів доступу процесу стосовно захищеного об'єкта, тобто при використанні критеріїв КД-1 і КА-1 достатньо реалізувати контроль доступу до окремо взятого елементу системи; базовий і повний рівні вимагають контролю атрибутів доступу користувача, при цьому користувачі можуть мати різні права доступу в кожному окремому елементі системи; абсолютний рівень вимагає контролю атрибутів доступу як користувача, так і процесу, це означає, що має здійснюватись не лише контроль доступу користувача до елементів системи, але й контролюється правомірність дій запущених користувачем процесів.

Повторне використання об’єктів — це послуга, що забезпечує коректність повторного використання об'єктів, що їх по черзі використовують різні користувачі та процеси, наприклад ділянки оперативної пам’яті та блоки (сектори) на жорсткому диску. Зазначені об’єкти належать до таких, через які може здійснюватися витік інформації. Послуга гарантує, що об'єкт після його надання новому користувачу чи процесу, не міститиме інформації від попереднього користувача чи процесу. Іншими словами, перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Окрім того, перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Послуга аналізу прихованих каналів забезпечує виявлення та закриття тих потоків інформації, що не контролюються іншими послугами. Рівні цієї послуги розподіляються відповідно до того, що виконується: лише виявлення (КК-1) і контроль (КК-2) або ще й перекривання (КК-3) таких прихованих каналів. Тобто, послуга КК-3 окрім виявлення та контролю за інформацією, що може

піддатись витоку через приховані канали, забезпечує також і внеможливлення такого витоку.

Послуга конфіденційності при обміні залежно від рівня забезпечує захист інформації від несанкціонованого доступу під час її передавання через незахищене середовище. Таку послугу реалізують здебільшого із застосуванням криптографічних механізмів. Таким чином, від надійності криптографічного алгоритму, за допомогою якого буде реалізована послуга, залежить рівень такої послуги, та відповідно, надійність захисту інформації від витоку на етапі її передавання чи обміну.

Далі пропонуємо розглянути критерії цілісності (рис. 2). Загалом критерії цілісності дають змогу оцінити комплекс засобів захисту (далі — КЗЗ) на предмет його спроможності захистити оброблювану інформацію від її несанкціонованої модифікації. До складу послуг безпеки, що забезпечують цілісність, належать: довірча цілісність, адміністративна цілісність, відкіт, цілісність під час обміну.

Рис. 2. Критерії цілісності

Послуги довірчої й адміністративної цілісності забезпечує підсистема керування доступом. Перша з них надає змогу користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. За допомогою другої адміністратор або спеціально авторизований користувач може керувати потоками інформації від користувачів до захищених об'єктів. Такі послуги дуже подібні до послуг довірчої й ад-

міністративної конфіденційності, разом з тим є певні відмінності, зокрема мінімальний рівень зазначених послуг цілісності потребує контролю атрибутів доступу користувача до захищеного об'єкта, а базовий і повний рівень — атрибутів доступу процесу.

Послуга повторного використання об’єктів надає можливість скасовувати операцію або послідовність операцій і повертати (відкочувати) захищений об'єкт до його попереднього стану. Рівні такої послуги розрізнюють на підставі множини операцій, для яких забезпечується відкіт.

Послуга забезпечення цілісності під час обміну відповідає за захист об'єктів від несанкціонованої зміни (модифікації) інформації, яку вони містять, під час їх передавання через незахищене середовище. Політика цілісності при обміні повинна визначати множину об'єктів і процесів інтерфейсу, до яких вона відноситься, рівень захищеності, що забезпечується послугою, а також спроможність користувачів і/або процесів керувати рівнем захищеності.

Наступним кроком слід розглянути критерії доступності (рис. 3). Такі критерії надають змогу оцінити здатність КЗЗ надавати послуги щодо забезпечення можливості використання комп’ютерної системи (далі — КС) у цілому, окремих її функцій чи ресурсів у певний проміжок часу, а також гарантувати спроможність КС функціонувати після відмови її компонентів. До послуг доступності належать: використання ресурсів, стійкість до відмов, «гаряча» заміна компонентів і відновлення після збоїв.

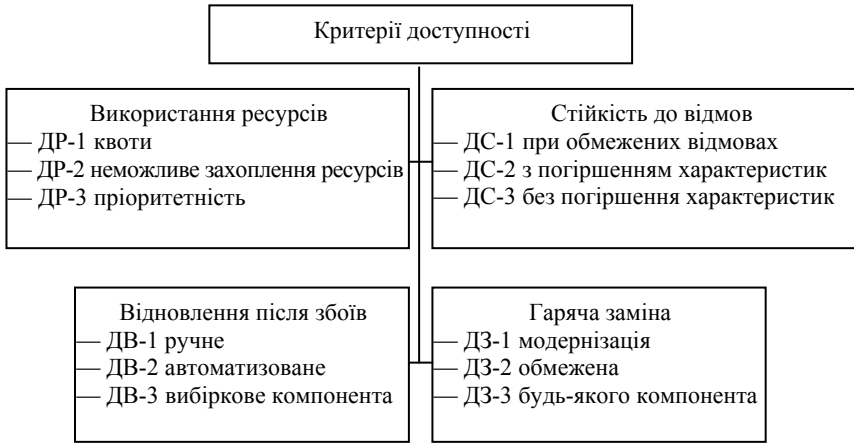

Рис. 3. Критерії доступності

Послуга використання ресурсів залежно від її рівня забезпечує квоти на використання відповідних ресурсів (ДР-1), унеможливлення захоплення ресурсів КС (ДР-2) або ж пріоритетність використання ресурсів (ДР-3). Політика використання ресурсів повинна визначати обмеження, що їх можна накладати на кількість даних об'єктів (обсяг ресурсів), що виділяються.

Послуга стійкості до відмов гарантує доступність інформації, окремих функцій чи елементів системи або ж КС у цілому після відмови одного з її компонентів. Рівні такої послуги визначаються, виходячи зі спроможностей КЗЗ забезпечити можливість функціонування КС залежно від кількості відмов, а також від кількості послуг, доступних після відмови.

Послуга відновлення після збоїв забезпечує повернення КС у відомий захищений стан, тобто, до контрольної точки після відмови або переривання обслуговування. Рівні такої послуги визначаються, виходячи зі ступеню автоматизації процесу відновлення.

Послуга так званої «гарячої» заміни забезпечує доступність КС (інформації, окремих функцій або КС у цілому) під час заміни окремих її компонентів. Рівні такої послуги визначаються залежно від повноти реалізації заміни.

Наступний блок критеріїв захищеності — критерії спостережності (рис. 4). Загалом цей комплекс критеріїв надає змогу оцінити КЗЗ щодо їх здатності надавати послуги, що змушують користувача КС відповідати за власні дії та забезпечують контроль за спроможністю КЗЗ виконувати свої функції. До послуг спостережності відносяться: реєстрація, ідентифікація й автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація й автентифікація під час обміну, автентифікація відправника, автентифікація одержувача.

Послуги реєстрації залежно від свого рівня, що ґрунтується на повноті контролю та складності засобів аналізу даних з журналів реєстрації, а також спроможності виявляти потенційні порушення, забезпечують контроль за небезпечними для КС діями шляхом реєстрації та аналізу подій, що впливають на безпеку.

Розподіл обов’язків між користувачами системи надає змогу знизити потенційні збитки, спричинені навмисними чи помилковими діями користувача, а також обмежити авторитарність керування. Рівні такої послуги визначаються на підставі вибірковості керування можливостями користувачів й адміністраторів.

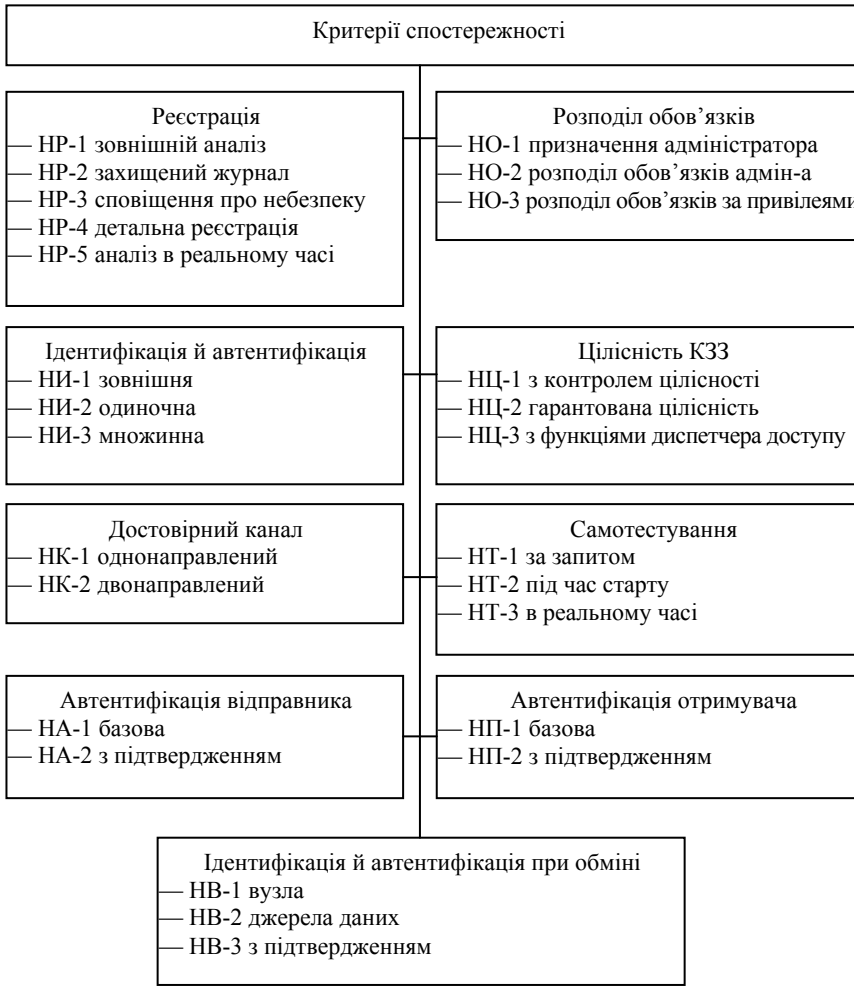

Рис. 4. Критерії спостережності

Ідентифікація й авентифікація користувачів надає КЗЗ можливість визначати й перевіряти особистість користувача, який намагається одержати доступ до КС. Рівні такої послуги визначаються залежно від того, чи є механізми автентифікації вбудованими чи зовнішніми, а також від кількості задіяних механізмів.

Завдяки послузі цілісності комплексу засобів захисту визначається ступінь здатності КЗЗ захищати самого себе та гарантувати свою спроможність керувати захищеними об'єктами. При цьому

у разі реалізації НЦ-1 та НЦ-2 повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ; при реалізації послуги НЦ-3 КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Послуга надання достовірного каналу забезпечує користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні такої послуги залежать від того, наскільки гнучко реалізовано можливість КЗЗ або користувача ініціювати захищений обмін.

Послуга самотестування надає змогу КЗЗ перевірити й на підставі такої перевірки гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні такої послуги визначаються залежно від того, чи виконуються тести в процесі запуску або ж штатної роботи.

Послуга автентифікації відправника надає змогу внеможливити відмову від авторства та однозначно встановити належність певного об'єкта конкретному користувачу. Рівні такої послуги визначаються на підставі можливості підтвердження результатів перевірки незалежною стороною.

Послуга автентифікації отримувача забезпечує внеможливлення відмови від отримання об'єкта і надає змогу однозначно встановити факт отримання певного об'єкта конкретним користувачем. Рівні такої послуги, аналогічно до попередньої послуги, визначаються на підставі можливості підтвердження результатів перевірки незалежною стороною.

Послуга ідентифікації й автентифікації під час обміну надає комплексам засобів захисту систем можливість ідентифікувати одне одного, перш ніж почати взаємодію. Залежно від повноти реалізації такої послуги визначаються її рівні.

Наступний блок критеріїв — критерії гарантій має сім рівнів, що є ієрархічними. Найнижчий рівень — 1, найвищий — 7. КС із певним рівнем гарантій має відповідати всім вимогам, визначеним для цього рівня (рис. 5).

Отже розглянемо вимоги, що висуваються до критеріїв гарантій. Вимоги до архітектури передбачають, що за умови їх виконання КЗЗ буде спроможним повністю реалізувати політику безпеки.

Вимоги до середовища розробки мають гарантувати, що процеси розробки та супроводження оцінюваної КС є цілковито керованими розробником.

Рис. 5. Вимоги критерію гарантій

Вимоги до процесу проектування (послідовності розробки) — за умови виконання таких вимог буде надано гарантії, що на кожному етапі розробки (проектування) існуватиме точний опис КС і що реалізація КС відповідатиме вихідним вимогам (політиці безпеки). Цей розділ містить підрозділи: вимоги до функціональних специфікацій (політика безпеки та її модель), вимоги до проекту архітектури, вимоги до детального проекту, вимоги до реалізації.

Вимоги до середовища функціонування гарантують, що КС постачається замовнику без несанкціонованих модифікацій і що вона буде інстальована та ініційована замовником так, як це було передбачено розробником.

Вимоги до документації забезпечують наявність та інформаційне наповнення розділів документації, де описано послуги безпеки, які реалізує КЗЗ, а також настанови адміністратору та користувачу щодо послуг безпеки.

Вимоги до випробувань КЗЗ регламентують дії розробника щодо надання програм, методик і результатів власних випробувань для перевірки незалежними експертами, а також демонструють, що виявлені під час випробувань слабкі місця захисту повністю усунено (це підтверджено додатковими випробуваннями).

Детальніше вимоги критеріїв гарантій доцільно розглядати безпосередньо під час вибору функціонального профілю захищеності інформаційної системи залежно від її класу та цільового ступеню захищеності.

Окремо слід зазначити, що для реалізації деяких послуг безпеки необхідною умовою є реалізація інших послуг. Виходячи з цього потрібно розуміти, що обов’язковими є послуги ідентифікації й автентифікації (НИ-1), без якої неможливо реалізувати систему розмежування доступу; надання достовірного каналу (НК-1), що необхідний для системи, в якій підсистема ідентифікації й автентифікації є внутрішньою (послуги НИ-2, НИ-3); розподілу обов'язків (НО-1), без якого неможливо реалізувати функції, що вимагають призначення адмі-

ністратора системи, зокрема адміністративного розмежування доступу, а також послуги доступності та деякі послуги спостережності; реєстрації (HP-1), за відсутності якої неможливо реалізувати послугу цілісності КЗЗ, що також є обов'язковою.

Обов'язковою умовою визначення функціонального профілю захищеності є клас системи. Сучасна нормативно-правова база, спираючись на архітектуру інформаційних систем, визначає три класи таких систем [6]:

клас 1 — одномашинний однокористувацький комплекс (окрема ПЕОМ без мережевих підключень);

клас 2 — локалізований багатомашинний багатокористувацький комплекс (локальна мережа);

клас 3 — розподілений багатомашинний багатокористувацький комплекс (інформаційна система, не локалізована на певній території, тобто, має незахищені канали передавання інформації).

Висновки. Аналіз критеріїв оцінки захищеності інформації дозволить керівнику сформувати оптимальний функціональний профіль захищеності інформації, що спиратиметься також на модель загроз і модель порушника безпеки. Чинна нормативно-правова база пропонує деякі стандартні функціональні профілі захищеності, втім до таких профілів, на нашу думку, слід підходити диференційовано та визначати їх з урахуванням вимог до конкретної інформаційної системи та захисту інформації, що в ній циркулює.

Питання методики формування функціональних профілів захищеності інформації в своїх працях розглядали зокрема Лєншин А.В., Буслов П.В. [7], Антонюк А.О. [8] та інші науковці. На зазначеній проблематиці будуть зосереджені й наші подальші дослідження. Зокрема буде запропоновано методику формування функціональних профілів захищеності інформації в інформаційних системах різних класів на підприємствах харчової промисловості.

Література

1. Маковський І.Ю. Аналіз вихідних даних для формування політики інформаційної безпеки на підприємстві: Економіка, управління та адміністрування. Житомир : Державний університет «Житомирська політехніка», 2020. вип. 1(91).

2. Бортник Н.П., Пєтков С.В. Загрози інформаційному ресурсу держави в контексті інформаційної та національної безпеки. Тези доповіді: ІТ право: Проблеми і перспективи розвитку в Україні. Львів–2016, С. 34-36.

3. Заячук, Я.І. Аналіз та оцінка ризиків інформаційної безпеки локальної обчислювальної мережі / Я.І. Заячук // Восточно-Европейский журнал передовых технологий. — 2012. — № 4/9(58). — С. 40-43.

4. Романюков, М.Г. Критерії оцінки ймовірності витоку інформації через технічні канали: Інформатика та математичні методи в моделюванні. — 2015. Том 5, №3. — С. 240-248.

5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

6. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 15.10.2008 № 172.

7. Лєншин А.В., Буслов П.В. Метод формування функціональних профілів захищеності від несанкціонованого доступу: Радіоелектронні і комп`ютерні системи. Харків, 2010. С. 77-81. ISSN: 2663-2012.

8. Антонюк А.О. Про деякі поняття захищеної інформації: Наукові записки НаУКМА//Комп'ютерні науки. Київ : Національний університет «Києво-Могилянська академія», 2000.

References

1. Makovskyi I.Iu. Analiz vykhidnykh danykh dlia formuvannia polityky informatsiinoi bezpeky na pidpryiemstvi: Ekonomika, upravlinnia ta administruvannia (Economics, management and administration). Zhytomyr : Derzhavnyi universytet «Zhytomyrska politekhnika», 2020. vyp. 1(91) [in Ukrainian].

2. Bortnyk N.P., Pietkov S.V. Zahrozy informatsiinomu resursu derzhavy v konteksti informatsiinoi ta natsionalnoi bezpeky. Tezy dopovidi: IT pravo: Problemy i perspektyvy rozvytku v Ukraini. Lviv–2016, s. 34-36 [in Ukrainian].

3. Zaiachuk, Ya.I. Analiz ta otsinka ryzykiv informatsiinoi bezpeky lokalnoi obchysliuvalnoi merezhi / Ya.I. Zaiachuk // Vostochno-Evropeiskyi zhurnal peredovykh tekhnolohyi (East European Journal of Advanced Technology). — 2012. — № 4/9(58). — S. 40-43 [in Ukrainian].

4. Romaniukov, M.H. Kryterii otsinky ymovirnosti vytoku informatsii cherez tekhnichni kanaly: Informatyka ta matematychni metody v modeliuvanni. — 2015. Tom 5, №3. — S. 240-248 [in Ukrainian].

5. Kryterii otsinky zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu. ND TZI 2.5-004-99. Zatverdzheno nakazom Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 28.04.1999 № 22 iz zminamy zghidno nakazu Administratsii Derzhspetszviazku vid 28.12.2012 № 806 [in Ukrainian].

6. Klasyfikatsiia avtomatyzovanykh system i standartni funktsionalni profili zakhyshchenosti obrobliuvanoi informatsii vid nesanktsionovanoho dostupu. ND TZI 2.5-005-99. Zatverdzheno nakazom Departamentu spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy vid 28.04.1999 № 22 iz zminamy zghidno nakazu Administratsii Derzhspetszviazku vid 15.10.2008 № 172 [in Ukrainian].

7. Lienshyn A.V., Buslov P.V. Metod formuvannia funktsionalnykh profiliv zakhyshchenosti vid nesanktsionovanoho dostupu: Radioelektronni i komp`iuterni systemy (Radio-electronic and computer systems). Kharkiv, 2010. S. 77-81. ISSN: 2663-2012 [in Ukrainian].

8. Antoniuk A.O. Pro deiaki poniattia zakhyshchenoi informatsii: Naukovi zapysky NaUKMA // Kompiuterni nauky (NaUKMA Scientific Notes // Computer Science). Kyiv : Natsionalnyi universytet «Kyievo-Mohylianska akademiia», 2000 [in Ukrainian].

Стаття надійшла до редакції 01.03.2020 р.

УДК 657.1:338
JEL Classification M 21, G 32
DOI 10.33111/EE.2020.44.ShilvinskaO_GlygaloN_KulykY

O. Shilvinska — *Accounting and Finance Lecturer, Cherkassy State Business College*

О.Л. Шільвінська — *викладач кафедри обліку та фінансів Черкаський державний бізнес коледж*

ORCID: https://orcid.org/0000-0002-6463-1050

N. Glygalo — *Accounting and Finance Lecturer, Cherkassy State Business College*

Н.А. Глигало — *викладач кафедри обліку та фінансів Черкаський державний бізнес коледж*

ORCID: https://orcid.org/0000-0003-4587-7298

Y. Kulyk — *Accounting and Finance Lecturer, Cherkassy State Business College*

Ю.М. Кулик — *викладач кафедри обліку та фінансів Черкаський державний бізнес коледж*

ORCID: https://orcid.org/0000-0002-0933-6884