https://www.proconference.org/index.php/usc/article/view/usc19-01-008
DOI: 10.30888/2709-2267.2023-19-01-008

УДК 004-049.5

OVERVIEW OF INFORMATION SECURITY RISKS ASSESSMENT FOR PERSONNEL

ОГЛЯД ПИТАННЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПЕРСОНАЛУ

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Yamnych A.B. / Ямнич А.Б.
аспірант / postgraduate
ORCID: 009-0005-7226-1896
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013

Анотація. *У статті розглядають оцінку та управління ризиками мережевої безпеки та персоналу як критичного активу. Аналіз критеріїв оцінювання персоналу та формування профілів працівників для ризик-менеджменту. Потенціал створення системи підбору критеріїв та ранжування профілів для зниження ризиків у мережевій безпеці компаній. Зазначено різні шляхи формування профілів кандидатів та потенційні похибки оцінювання. Профілювання персоналу - ключовий аспект інформаційної безпеки. Описано контроль доступу, процес ідентифікації та автентифікації. Чотири моделі контролю доступу: обов'язковий, за роллю, дискреційний та на основі правил. Представлена порівняльна схема критеріїв позиції та профілів кандидатів для оцінювання ризиків.*

Ключові слова: *Оцінка ризиків мережевої безпеки, критерії оцінювання персоналу, формування профілів працівників, контроль доступу, моделі контролю доступу, інформаційна безпека компаній.*

Вступ.

У зв'язку зі зростаючими ризиками, пов'язаними зі взаємодією людського персоналу з інформацією, пропонуються заходи, що можуть визначати ризики під час надавання доступу до інформації конкретним особам, з урахуванням їхньої відповідальності та рівня доступу. Впровадження управління ризиками в галузі інформаційної безпеки стало предметом досліджень вчених, які

зосереджуються на важливості людських активів інформаційних систем [1-2].

Необхідність створення систематизованих методів та засобів підбору та оцінювання персоналу породжує наукове протиріччя, оскільки науково-методичний апарат не завжди є адекватним. Тому актуальною є розробка системи оцінювання ризиків інформаційної безпеки, які виникають під час доступу до інформаційних ресурсів компанії, а також формування критеріїв для отримання цього доступу як засобу ефективного підбору персоналу через організацію системи оцінки ризиків [3-6].

Для досягнення більш гнучкого та ефективного контролю доступу до інформаційних ресурсів компанії пропонується розробити комплексну систему оцінки ризиків інформаційної безпеки для персоналу під час розмежування доступу. Це дозволить підвищити рівень безпеки і знизити ймовірність кібер-атак та несанкціонованого доступу до важливої інформації компанії.

1 Персонал, як критичний актив.

Оцінка та управління ризиками мережевої безпеки була створена як наукова галузь приблизно 30-40 років тому. Тоді ж були розроблені принципи та методи, для розробки концепції, оцінки та управління ризиками мережевої безпеки. Ці принципи та методи досі є базовими для цієї галузі і сьогодні, але буквально протягом останньої декади було надбано чимало теоретичних напрацювань та практичних моделей та процедур [2, 7].

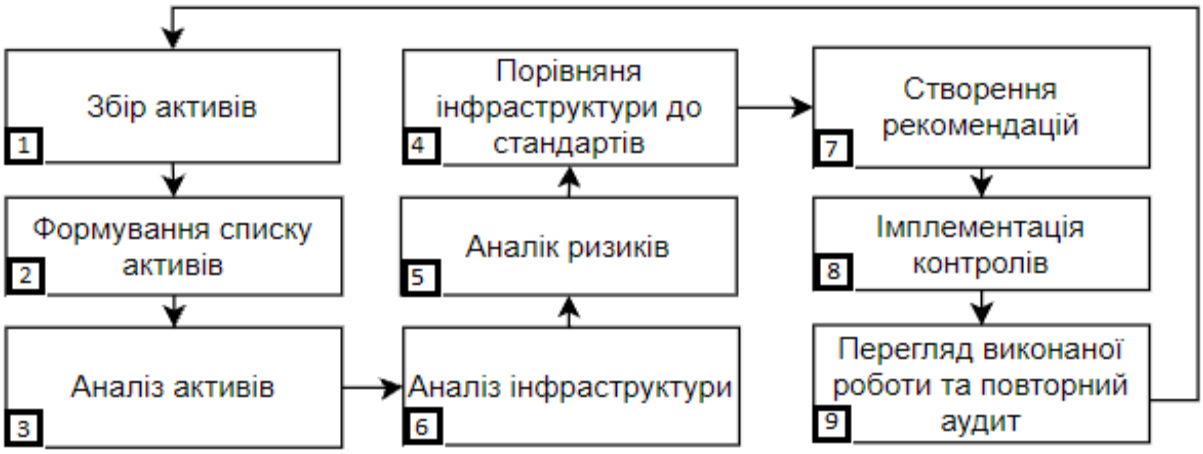

Рисунок 1 – Схема визначення та вирішення/прийняття ризиків мережевої безпеки

Джерело: [2,7]

Першим етапом є збір активів. Щоб зрозуміти ризик, необхідно знайти найцінніші активи компанії. Часто це сервери, комунікаційні мережі та інформаційні системи, послуги, політики тощо. Персонал також зараховують до складу активів, оскільки він часто є одним із найбільш вразливих та найцінніших активів одночасно.

1.1 Аналіз персоналу як критичного активу компанії. При формуванні ризиків, пов'язаних з обладнанням та інфраструктурою компанії, звертають увагу на технічні характеристики та вимоги. Це підтверджується сертифікатами якості. Але оцінка персоналу вимагає іншого підходу, оскільки люди мають унікальні навички, які не підтверджуються сертифікатами. Людський персонал є унікальним набором якостей та досвіду, що робить його не порівнюваним з іншими активами.

1.2 Критерії оцінювання персоналу. При прийомі на роботу або підвищенні в організації, змінюється вплив людини, тому потрібні певні критерії відбору. Критерії можуть змінюватися та мати різну важливість залежно від позиції. Наприклад, для охоронця важлива відповідальність, а для розробника програмного забезпечення - освіта.

1.3 Формування профілю працівника. Усі кандидати мають унікальний профіль з позитивними та негативними факторами. Складаючи критерії та порівнюючи профілі, можна визначати рівень довіри для отримання певної позиції та оцінювати ризики для компанії.

2 Методи та засоби оцінювання персоналу.

Для підбору кандидатів різні компанії використовують різні шляхи для складання профілю кандидатів [8]. Перший та найпростіший спосіб це збирання резюме. Він дозволяє швидко обробити велику кількість кандидатів маючи базову інформацію про них. Після цього багато компаній проводять онлайн тестування для визначення рівня технічних навичок (рис. 2).

Замість автоматизованого тестування, для визначення технічних навичок, проводяться технічні інтерв’ю. Після визначення рівня технічної підготовки проводиться інтерв’ю з кандидатом під час якого компанія пробує визначити

наявність особистих якостей та недоліків кандидата.

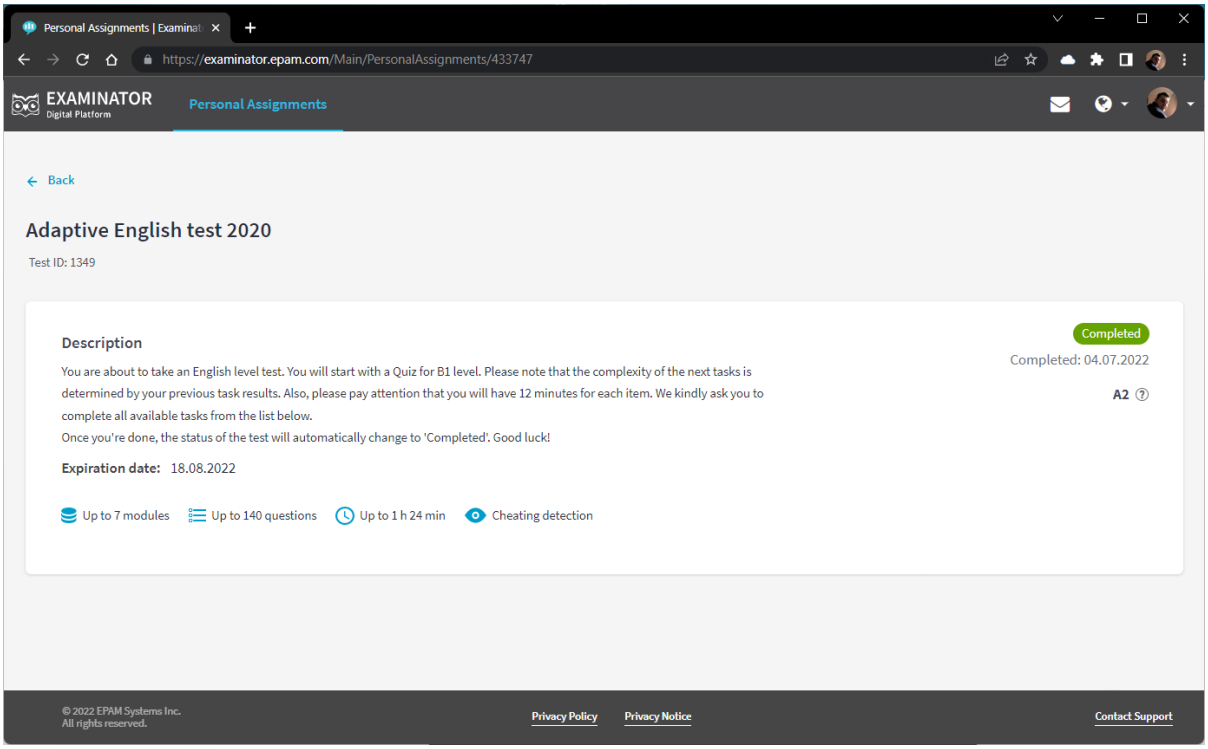

Рисунок 2 – EPAM Examinator Digital Platform – платформа для комплексного тестування для кандидатів в компанію EPAM Systems

Джерело: [8]

Крім інтерв'ю та тестування компанії також проводять різні опитування та анкетування для збору інформації про кандидатів а також вже найнятих співробітників. Це все є частиною аудиту персоналу.

2.1 Потенційні похибки під час оцінювання персоналу. При оцінюванні персоналу можуть виникати помилки зі сторони кандидата і компанії. Кандидат може навмисно або ненавмисно спотворити інформацію у своєму профілі, що робить його профіль недостовірним. Персонал компанії також може зіграти роль у спотворенні профілю кандидата, або збирати недостатньо інформації для об'єктивного порівняння. Помилки також можуть виникнути при підборі критеріїв та визначенні їх важливості, що може призвести до неправильного ранжування кандидатів.

2.2 Роль профілювання. Людський персонал є найважливішим активом підприємства з погляду інформаційної безпеки, і його аудит вимагає особливих

методів. Для кожної позиції в компанії використовуються свої критерії з різним рівнем важливості. Кожен кандидат має унікальний профіль, і відповідність профілів до критеріїв дозволяє здійснювати порівняння кандидатів. На основі профілів також визначається рівень довіри до кандидатів, що є ключовим для прийняття рішень щодо контролю доступу. Існують різні методи оцінки кандидатів, але вони мають свої недоліки [9].

3 Зв'язок між розмежуванням доступу до інформаційних ресурсів компанії та аналізом оцінки персоналу

3.1 Поняття розмежування доступу. Контроль доступу – процес ідентифікації та автентифікації осіб для надання доступу до певних ресурсів. Моделі контролю доступу включають чотири основних типи: Модель обов’язкового контролю доступу (MAC); Модель контролю доступу за роллю (RBAC); Модель дискреційного контролю доступу (DAC); Модель контролю доступу на основі правил (RBAC or RB-RBAC) [10].

3.2 Моделі контролю доступу. Модель обов’язкового контролю доступу (MAC) забезпечує контроль доступу власникам та авторизованим менеджерам компанії. Застосовуються дві моделі MAC: Biba, орієнтована на цілісність інформації, та Bell-LaPadula, орієнтована на конфіденційність. Модель контролю доступу за роллю (RBAC) передбачає контроль доступу на основі посади, що займає особа. Призначення на певну посаду автоматично надає необхідні дозволи. Модель дискреційного контролю доступу (DAC) дозволяє користувачам контролювати доступ до об'єктів, які вони володіють. Ця модель може бути менш обмежувальною, але має певні недоліки. Модель контролю доступу на основі правил (RBAC or RB-RBAC) дозволяє динамічно присвоювати користувачам ролі на основі визначених правил.

3.3 Схема порівняння критеріїв позиції та профілів кандидатів. На рис. 3 зображено авторську схему порівняння критеріїв позиції та профілів кандидатів. На початку схеми зображено позицію: список критеріїв які вимагаються та їхнє схематичне співвідношення між собою. А також необхідний рівень довіри. Далі є блоки кандидатів, які представлені для

порівняння з позицією та між собою. В кожного кандидата є список якостей за критеріями які є затребуваними позицією, а також рівень довіри.

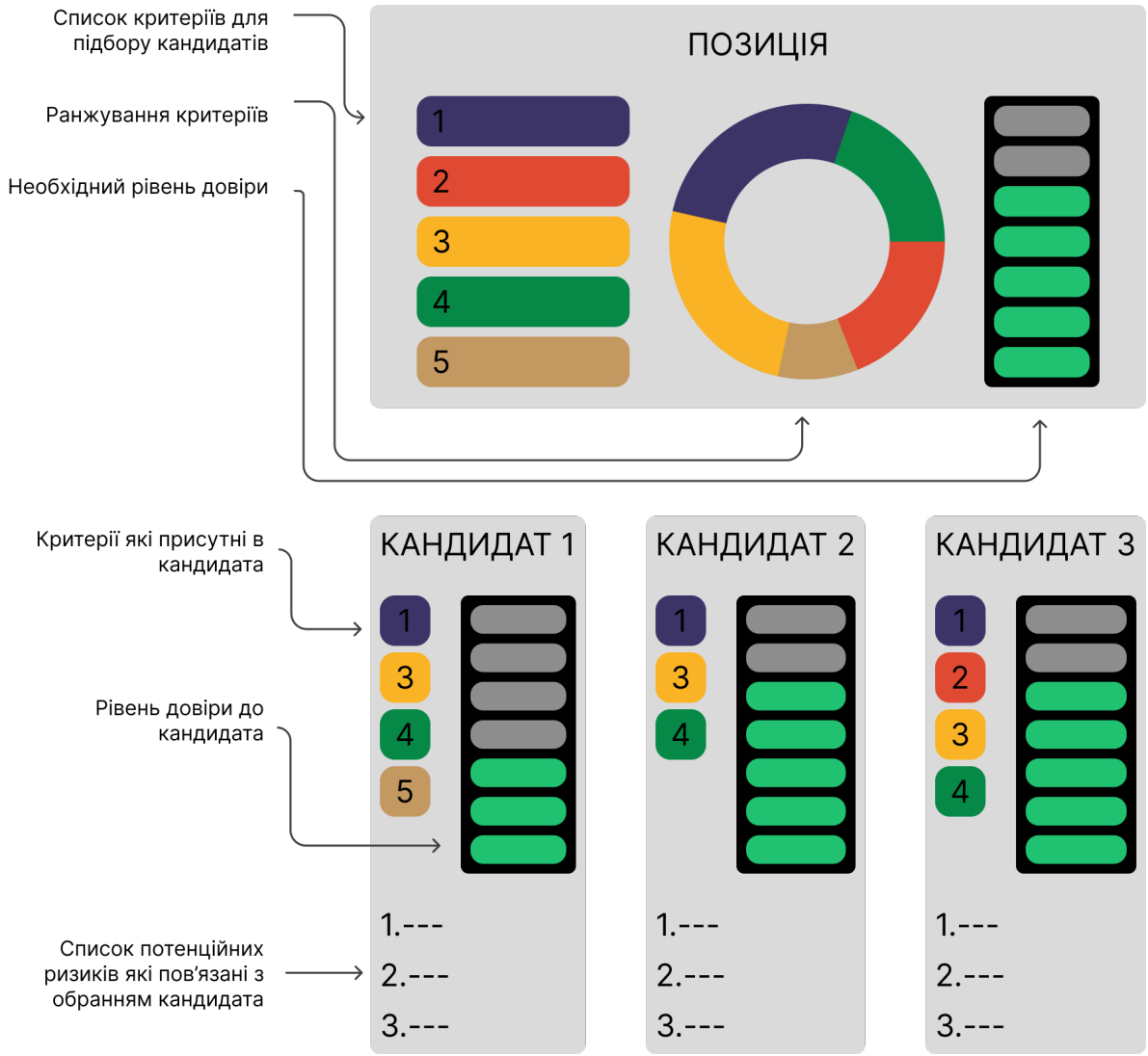

Рисунок 3 – Схема порівняння критеріїв позиції та профілів кандидатів

Авторська розробка

На основі порівняння кандидатів до позиції до кожного кандидата складається список потенційних ризиків, які пов'язані з його обранням на позицію.

Висновки.

У цій статті аналізується розробка системи оцінювання ризиків ІБ під час доступу до інформаційних ресурсів компанії та складання критеріїв для такого доступу. Система допомагає ефективно керувати доступом до інформації,

оцінюючи ризики ІБ та враховуючи критерії для отримання доступу. Важливість аналізу персоналу як критичного активу компаній та формування профілів працівників для ефективного ризик-менеджменту також підкреслюється. Використання профілювання є важливим для об'єктивного порівняння кандидатів та контролю доступу. Моделі контролю доступу, такі як MAC, RBAC та DAC, допомагають забезпечити безпеку і контроль доступу до інформації. Запропонована схема порівняння критеріїв позиції та профілів кандидатів допомагає зробити обґрунтовані вибори кандидатів для певних позицій.

Література:

1. Стандартизація, сертифікація, метрологія та управління якістю [Електронний ресурс] // Чернівецький національний університет імені Юрія Федьковича. – 2022. – Режим доступу до ресурсу: https://archer.chnu.edu.ua/xmlui/bitstream/handle/123456789/3880/%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D0%A1%D0%A1%D0%9C%D1%82%D0%B0%D0%A3%D0%AF.pdf?sequence=1&isAllowed=y.

2. Таченко І. А. Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки / І. А. Таченко, Т. І. Коробейнікова, С. М. Захаченко // Scientific Collection «InterConf», (84): with the Proceedings of the 5th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p. – С. 417-432. – ISBN 978-88-32012-34-7. DOI 10.51582/interconf.7-8.11.2021.

3. Кобрин М. В. Метод визначення цінності інформаційних активів організації [Електронний ресурс] / Максим Виталійович Кобрин. – 2015. – Режим доступу до ресурсу: https://doi.org/10.18372/2410-7840.16.7541.

4. Пузиренко О. Г. Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах / О. Г. Пузиренко, С. О. Івко, О. О. Лаврут, О. К. Климович // Системи обробки інформації. - 2015. - Вип. 3. - С. 75-79. - Режим доступу:

http://nbuv.gov.ua/UJRN/soi_2015_3_17.

5. Родін Є. С. Процесні підходи до моделювання у сфері управління ризиками інформаційної безпеки / Є. С. Родін // Математичні машини і системи. - 2012. - №4. - С. 142-148. - Режим доступу: http://nbuv.gov.ua/UJRN/MMS_2012_4_18

6. Шевцов І. Оцінка ризиків та створення ефективної системи внутрішнього контролю [Електронний ресурс] / Ігор Шевцов. – 2019. – Режим доступу до ресурсу: https://blog.liga.net/user/ishevtsov/article/33611.

7. Tachenko I. The basic aspects of assessment and risk remediation technological chain / I. Tachenko, T. Korobeinikova // "Information protection and information systems security" : Materials of VIII-th International Scientific and Technical Conference, November 11 – 12, 2021. – Lviv: NULP, 2021 – С. 17-19. (вітч. міжнар. конф. – тези)

8. Психометричне профілювання [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://ourdataourselves.tacticaltech.org/posts/psychometric-profiling-uk/.

9. Методи ранжування критеріїв в задачі оптимізації потокорозподілу інженерної мережі [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://repositary.knuba.edu.ua:8080/xmlui/handle/987654321/788.

10. Контроль доступу (Access control) до інформації як один із ключових елементів інформаційної безпеки [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://bsoprivacygroup.com/gdpr-personal-data-access-control/.

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.

Стаття надіслана: 25.07.2023 р.