https://www.sworldjournal.com/index.php/swj/article/view/swj20-01-024
DOI: 10.30888/2663-5712.2023-20-01-024

УДК 004-049.5

INFORMATION SECURITY RISKS ASSESSMENT FOR PERSONNEL

ОЦІНКА 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: 0009-0005-7226-1896
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013

Анотація. *В статті розглядається оцінку та управління ризиками мережевої безпеки з фокусом на аналіз персоналу як критичного активу. Розглянуто критерії оцінювання персоналу, важливість їх відповідності та необхідність формування профілів працівників для ефективного ризик-менеджменту. Дослідження має потенціал створення системи підбору критеріїв для конкретних позицій та ранжування профілів для зниження ризиків у мережевій безпеці компаній. Зазначено різні шляхи формування профілів кандидатів, висвітлено потенційні похибки оцінювання. Профілювання персоналу розглядається як ключовий аспект забезпечення інформаційної безпеки компаній. Описано контроль доступу, процес ідентифікації та автентифікації осіб. Описано чотири моделі контролю доступу: обов'язковий, в контексті визначеної ролі, дискреційний та на основі правил. Приведено порівняльну схему критеріїв позиції та профілів кандидатів для оцінювання потенційних ризиків.*

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

Вступ.

Розвиток систем обробки, зберігання та передачі інформації як частини інформаційних ресурсів компанії, а також, потенційні кібер-загрози від суб'єктів таких систем [1] породжує впровадження комплексних засобів розмежування та контролю доступу шляхом оцінки ризиків інформаційної безпеки (ІБ) з точки зору персоналу. Відомо, що одним із найбільш критичних активів системи є людський персонал [2], аудит якого здійснюється для оцінки ризиків ІБ. У зв'язку з ризиками, що зумовлені взаємодією людського персоналу з інформацією, пропонуються заходи, які можуть визначати ризики під час надавання доступу до інформації конкретним особам із урахуванням рівня відповідальності, що покладається на них разом із доступом до цієї інформації. Впровадження управління ризиками у галузі ІБ стало предметом досліджень таких вчених: Кобрина М. В. [3] О.Г. Пузиренка [4], Є.С. Родіна [5], Шевцова І [6] та багатьох інших науковців, які серед різних аспектів особливу увагу приділяють людським активам інформаційної системи шляхом розв'язання задач аудиту.

Комплексна система оцінки ризиків ІБ для персоналу полягає у ранжуванні відповідальності для розмежування доступу до інформаційних ресурсів компанії, що призводить до створення критеріїв для отримання доступу.

Між необхідністю створення систематизованих методів та засобів підбору

та оцінювання персоналу і водночас відсутністю адекватного науково-методичного апарату виникає наукове протиріччя. Отже, актуальним є вирішення наукової задачі розробки системи оцінювання ризиків ІБ, які виникають під час доступу до інформаційних ресурсів компанії; та складання критеріїв для отримання цього доступу як засобу реалізації якісного підбору персоналу шляхом організації системи оцінки ризиків ІБ.

Стаття присвячена подальшому розвитку інформаційних процесів оцінки ризиків ІБ для персоналу в галузі побудови захищених інформаційних середовищ. Таким чином, з'являється можливість досягти більш гнучкого та ефективного контролю доступу до інформаційних ресурсів. Для цього планується розробити комплексну систему оцінки ризиків ІБ для персоналу під час розмежування доступу до інформаційних ресурсів 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].

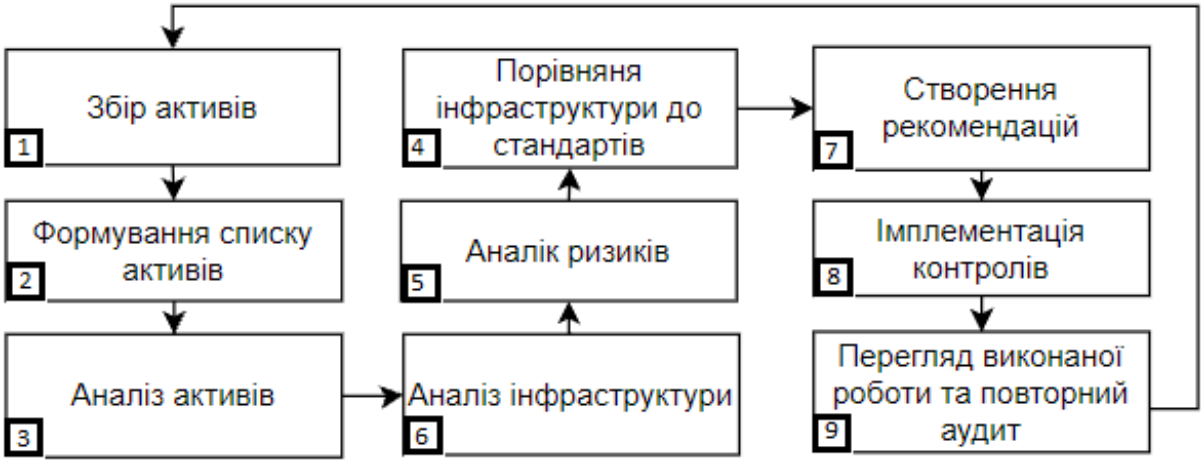

Рисунок 1 – Схема визначення та вирішення/прийняття ризиків мережевої безпеки

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. Під час формування ризиків пов'язаних із обладнанням та інфраструктурою як активів компанії, до уваги беруться технічна відповідність характеристик та вимоги до поставлених задач. Враховуються сертифікати якості від виробника, який виступає гарантом цієї якості і відповідає за неї [1]. Крім того існують стандарти сертифікації, яке

воно може отримати, якщо задовольняє певні вимоги. З людським персоналом подібне зустрічається під час оцінки навичок і знань за допомогою централізованої системи освіти, яка виступає гарантом створюючи стандарти і системи оцінювання за стандартами. Проте люди володіють значно більшою кількість навичок і вмінь, які не підтверджуються сертифікатами. Також обладнання підлягає ремонту чи заміні на ідентичне справне, що є неможливим коли мова йде про заміну персоналу. Кожна людина, як актив компанії є унікальним набором навичок, вмінь, досвіду, характеру, а також і недоліків. З цього випливає, що людський персонал, як актив, не може порівнюватись з іншими активами і потребує іншої системи

1.2 Критерії оцінювання персоналу. Під час прийому на роботу чи підвищення або будь якої іншої зміни позиції особи (кандидата) в межах організації змінюється вплив людини в межах цієї організації, за рахунок здобування нових обов'язків та отримання доступу до інформації. Відповідно до того людина повинна бути відібрана за певними критеріями.

Список критеріїв є відносним і змінюється, також, варіюється важливість відповідності різним критеріям, адже одні якості є важливішими за інші на різних позиціях. Наприклад, позиція охоронця є дуже відповідальною і вимагає велику кількість різних особистих якостей, оскільки кандидат може отримувати доступ до фізичних сховищ інформації і тому має бути дуже організованим, зосередженим, уважним тощо. Проте, в межах критерію «Освіта» кандидат немає таких високих вимог як наприклад розробник програмного забезпечення. Водночас розробник працює тільки в межах своєї команди і свого проекту і не має високого рівня допуску.

В перспективі даного дослідження доцільно створити систему підбору критеріїв для конкретної позиції, їх порівняння та ранжування. За допомогою цієї системи можна буде створювати точніший перелік вимог до кандидатів для їх якіснішого підбору.

1.3 Формування профілю працівника. Критерії для позицій сукупно складають ідеального кандидати для неї. Проте люди це не тільки набір позитивних якостей. В них, як в кандидатів, в кожного є свої недоліки, які можуть бути не тільки в межах вибраних категорій. Кримінальне минуле, податкова історія, соціальний статус, психологічний портрет та багато інших також відрізняють між собою кандидатів. Сукупність позитивних та негативних факторів кожного кандидата формують його особистий профіль [8]. Як вже зазначалось раніше, усі кандидати є унікальними, відповідно і їхні профілі також є унікальними. Проте складаючи критерії позиції та відповідність певного профілю цим критеріям з'являється можливість вираховувати різницю відповідності профілів до критеріїв та порівнювати ці профілі між собою. Також враховуючи різні рівні відповідальності різних позицій для профілів є можливість визначати рівень довіри та зазначати необхідний рівень довіри для отримання позиції. Порівняння відповідності критеріям та рівнів довіри є необхідним для оцінки ризиків адже різні показники в різних кандидатів це різні потенційні ризики для компанії і вона вже може вирішувати які для неї буде вигідніше прийняти.

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).

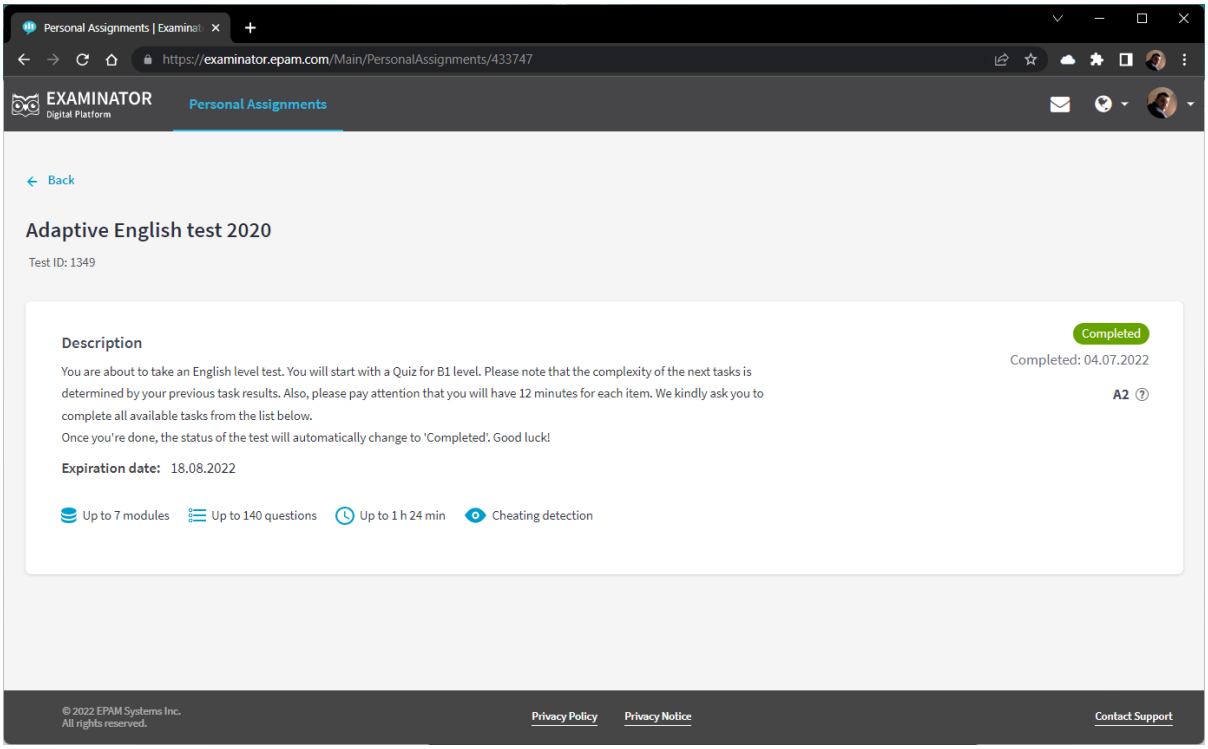

Рисунок 2 – EPAM Examinator Digital Platform – платформа для комплексного тестування для кандидатів в компанію EPAM Systems

Джерело: [8]

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. 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. Перше що варто вказати, це людський фактор, як зі сторони кандидата так і зі сторони компанії. Зі сторони кандидата можливе неправильна подача інформації до свого профілю – навмисна чи ненавмисна, що робить його профіль не відповідаючим дійсності. Зі сторони компанії людський грає роль коли опрацюванням інформації про кандидата займається персонал. Персонал може так само навмисно чи не навмисно спотворити профіль кандидата. Крім того персонал може зібрати недостатньо інформації необхідної для об'єктивного порівняння кандидатів до вимог чи визначення рівня довіри. Це ж стосується і автоматизованих методів збору інформації – анкетування та опитування.

Підбір критеріїв та визначення їх важливості також може бути зроблено невірно що може призвести до похибок при підборі кандидатів та відсіяти хороші варіанти через неправильне ранжування критеріїв [9]. Наприклад особа на позицію дизайнера яка матиме доступ тільки до комунікаційних ресурсів компанії таких як корпоративна пошта може бути відкинута через кримінальне минуле, хоча в розрізі ІБ такий кандидат не становить високих загроз.

2.2 Роль профілювання. Людський персонал є одним з найважливіших активів підприємства в розрізі інформаційної безпеки. Його неможливо прирівнювати до інших видів активів і відповідно для його аудиту необхідно використовувати інші методи. Для кожної позиції в компанії є свій підбір критеріїв, які між собою відрізняються за рівнем важливості. Так само і кожен кандидат відрізняється унікальним набором якостей, вмінь та недоліків які формують його профіль. Відповідність профілів до критерію дає можливість здійснювати порівняння кандидатів. На основі профілів також базується рівень довіри до кандидатів що є ключовим для прийняття рішень в сфері контролю доступу. Зараз використовуються різні методи оцінки кандидатів проте вони мають недоліки.

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

3.1 Поняття розмежування доступу. Контроль доступу – в загальному розумінні це процес ідентифікації осіб, які виконують певну роботу, а також їхня автентифікація в контексті отриманих результатів ідентифікації [10]. І тільки автентифікованим особам можуть надаватися інструменти доступу до певних засобів (наприклад пароль доступу до комп’ютера чи певної системи). У світі захисту інформатизації, це можна розглядати як надання індивідуального дозволу на потрапляння в мережу через ім’я користувача та пароль, що дозволяє їм отримувати доступ до файлів, комп’ютерів чи іншого апаратного чи програмного забезпечення, яке вимагає особа з ціллю виконання поставлених компанією завдань.

Отже, в контексті надання особі потрібного рівня доступу до інформації, необхідно розглянути моделі контролю доступу, які діляться на чотири основні види [7]:

- Модель обов’язкового контролю доступу (Mandatory Access Control (MAC));
- Модель контролю доступу, в контексті визначеної ролі (посади) (Role Based Access Control (RBAC));
- Модель дискреційного контролю доступу (Discretionary Access Control (DAC));
- Модель контролю доступу на основі (встановлених) правил (Rule Based Access Control (RBAC or RB-RBAC)).

Mandatory Access Control (MAC). Модель обов’язкового контролю доступу надає право контролю доступу лише власникам компанії та авторизованим менеджерам компанії. Це означає, що кінцевий користувач не має контролю над будь-якими налаштуваннями в рамках інформаційної системи. Зараз є дві моделі безпеки, пов’язані з MAC:

– Biba;
– Bell-LaPadula.

Модель *Biba* орієнтована на цілісність інформації, тоді як модель *Bell-LaPadula* орієнтована на конфіденційність інформації.

Biba – це модель, в рамках якої користувач з низьким рівнем допуску до інформації може ознайомлюватися з інформацією більш високого рівня (так званий «read up»), а користувач з високим рівнем допуску має можливість ознайомлювати, в письмовому вигляді, користувачів з нижчим рівнем допуску з інформацією вищого рівня (так званий «write down»). Модель Biba зазвичай використовується в компаніях, де працівники нижчих рівнів можуть читати інформацію вищого рівня, а керівники можуть надавати інформацію в письмовому вигляді з ціллю інформувати працівників нижчого рівня.

Bell-LaPadula – це модель яка визначає рівні доступу в залежності від ступеня конфіденційності інформації. Модель Bell-LaPadula передбачає, що користувач з високим рівнем допуску має можливість розкривати інформацією лише користувачам на цьому ж рівні і не нижче (так званий «write up»), але також може ознайомлюватися з інформацією на нижчих рівнях допуску (так званий «read down»). Таку модель зазвичай використовують в державних або військових установах. Наприклад, в деяких арміях світу, можливо зустріти градацію конфіденційності за рівнями секретності, конфіденційності та доступності (наприклад: «дуже секретно», «секретно», «конфіденційно», «у відкритому доступі»).

Role Based Access Control (RBAC) Контроль доступу в контексті визначеної ролі забезпечує контроль доступу на основі посади, яку займає окрема особа в компанії. Отже, наприклад, замість отримання додаткових дозволів на доступ до певної інформації, яка може доступна тільки працівникам безпеки, особа отримує такий доступ автоматично в момент призначення його на посаду, пов’язану із забезпеченням безпеки компанії. Зайняття певної посади в рамках компанії автоматично передбачає надання дозволів на доступ до інформації на певному рівні. Ця модель є також доволі практичною для використання компаніями, як володіють інформацією, що не може бути доступною для всіх працівників.

Discretionary Access Control (DAC) Дискреційна модель контролю доступу до інформації є найменш обмежувальною моделлю порівняно з найбільш обмежувальною моделлю Mandatory Access Control. DAC дозволяє окремій особі здійснювати повний контроль над будь-якими об’єктами, якими вона володіє, а також програмами, пов’язаними з цими об’єктами. Така модель може мати слабкі сторони, які полягають в тому, що така модель дає кінцевому користувачеві повний контроль для встановлення параметрів рівня безпеки для інших користувачів, що може призвести до того, що такі кінцеві користувачі в рамках компанії матимуть більш високі привілеї, ніж вони повинні мати.

Rule Based Access Control (RBAC or RB-RBAC) Контроль доступу на основі правил – модель, яка передбачає наявність технічних інструментів, які передбачають можливість динамічного присвоєння користувачам ролей на основі критеріїв, визначених, наприклад, системним адміністратором Компанії

або іншим відповідальним спеціалістом в сфері інформаційної безпеки. Якщо будь-кому надається доступ до бази даних лише протягом певних годин дня, то такий доступ повинен регламентуватися певними правилами або ж затвердженим порядком, який є обов'язковим для погодження всіма працівниками компанії.

3.2 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.

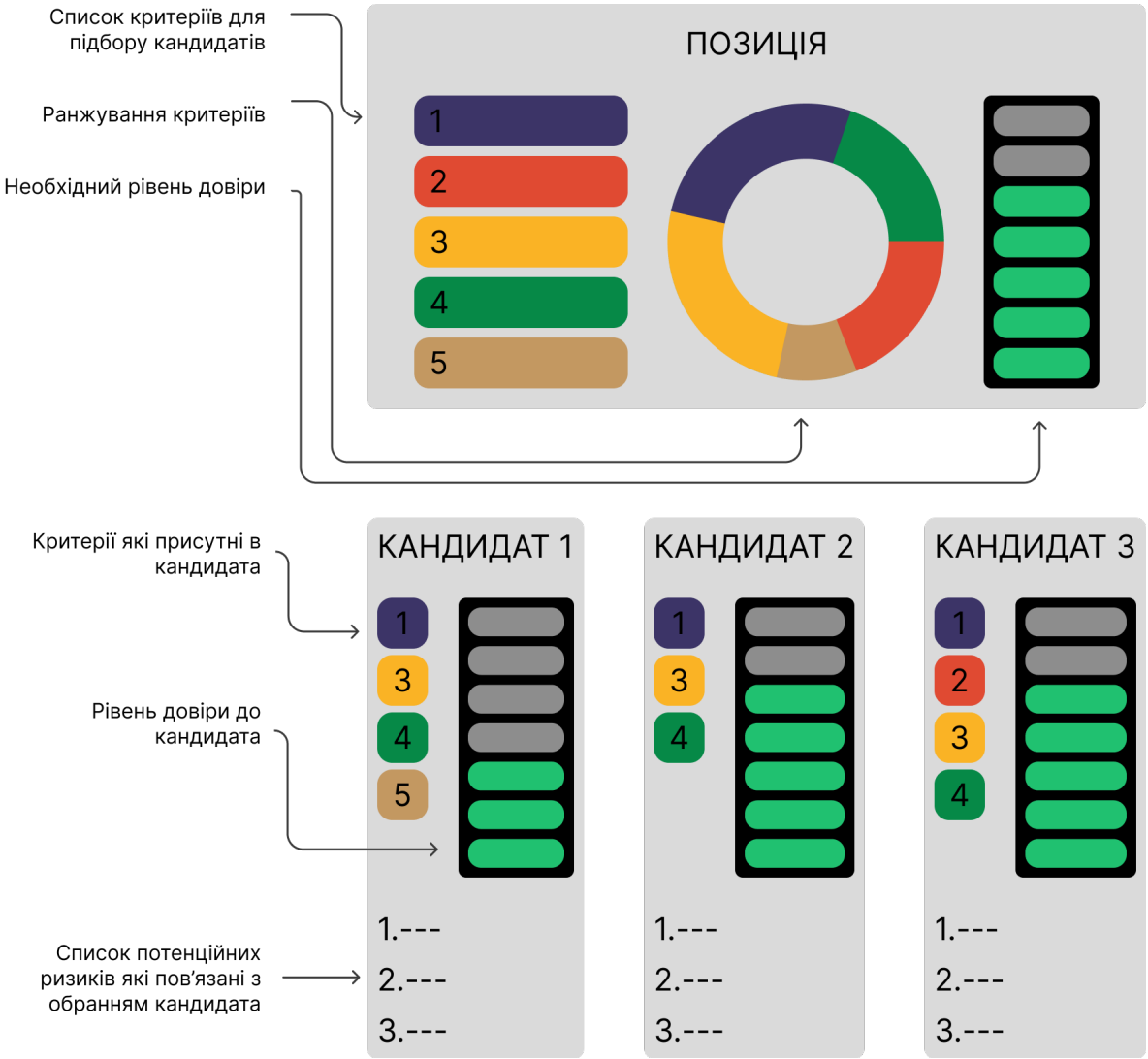

Рисунок 3 – Схема порівняння критеріїв позиції та профілів кандидатів
Авторська розробка

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 проведено аналіз вирішення наукової задачі розробки системи оцінювання ризиків ІБ, які виникають під час доступу до інформаційних ресурсів компанії та складання критеріїв для отримання цього доступу як засобу реалізації якісного підбору персоналу шляхом організації системи оцінки ризиків ІБ.

Комплексна система оцінки ризиків інформаційної безпеки для персоналу під час розмежування доступу до інформаційних ресурсів компанії дозволить підвищити ефективність управління доступом до інформації шляхом оцінювання ризиків ІБ та з урахуванням критеріїв для отримання цього доступу.

Стаття розглядає оцінку ризиків ІБ для персоналу та розмежування доступу до інформаційних ресурсів компаній. Запропоновані заходи дозволяють створити критерії для отримання доступу. Розвиток такої системи є актуальним і сприятиме покращенню контролю доступу.

Підкреслено важливість аналізу персоналу як критичного активу компаній та формування профілів працівників для ефективного ризик-менеджменту. Виробництво комплексної системи оцінки ризиків ІБ є актуальним і сприятиме кращому контролю доступу. Оцінювання персоналу – складний процес, що включає різні методи: збір резюме, онлайн тестування, технічні інтерв'ю, анкетування. Проте існують потенційні похибки, пов'язані з людським фактором та неправильним підбором критеріїв. Використання профілювання є важливим для об'єктивного порівняння кандидатів та контролю доступу. Зв'язок між розмежуванням доступу та оцінкою персоналу полягає в тому, що ефективне контролювання доступу до інформаційних ресурсів компанії допомагає підвищити об'єктивність аналізу оцінки персоналу. Моделі контролю доступу, такі як MAC, RBAC та DAC, допомагають забезпечити безпеку і контроль доступу до інформації.

Запропонована автором 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/.

Abstract. *The article discusses the assessment and management of network security risks with a focus on personnel analysis as a critical asset. Criteria for personnel evaluation, their relevance, and the need to create employee profiles for effective risk management are explored. The research has the potential to develop a criterion selection system for specific positions and rank profiles to reduce risks in company network security. Various approaches to candidate profiling are highlighted, and potential assessment errors are discussed. Profiling personnel is considered a key aspect of ensuring company information security. Access control, the process of identification, and authentication of individuals are described. Four models of access control are outlined: mandatory, role-based, discretionary, and rule-based. A comparative scheme of position criteria and candidate profiles is provided for potential risk assessment..*

Key words:*. Risk assessment of network security, personnel evaluation criteria, employee profiling, access control, access control models, and information security of companies.*

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.
Стаття надіслана: 25.07.2023 р.