УДК 004.056.5:005.8 **DOI:10.30837/rt.2024.4.219.01**

Т.І. КОРОБЕЙНІКОВА, канд. техн. наук, А.Б. ЯМНИЧ

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ПЕРСОНАЛУ ПІД ЧАС РОЗМЕЖУВАННЯ ДОСТУПУ ДО РЕСУРСІВ КОМПАНІЇ

Вступ

Персонал компанії є одним із критичних активів і водночас однією з найслабших ланок її інформаційної безпеки (ІБ), тому у сучасних установах на регулярній основі відбувається його аудит з метою оцінювання ризиків безпеки [1–3]. Впровадження оцінювання ризиків у галузі інформаційної безпеки компаній уже давно стало актуальним предметом наукових праць вітчизняних та закордонних дослідників, які наголошують на важливості людського фактора в безпеці функціонування інформаційних систем [4–5]. Як зазначають автори одного з найактуальніших українських досліджень впливу людини на інформаційну безпеку, «натепер рівень інформаційних атак, які включають людський чинник, значно збільшується» [2]. Нині найбажанішим здобутком від атак на інформаційні системи компанії є персональні дані її працівників, облікові записи користувачів робочих станцій, комерційна таємниця, бази даних, внутрішня переписка, дані банківських рахунків тощо. З метою попередження атак та виявлення потенційних загроз для інформаційних ресурсів компанії потрібно навчитися застосовувати різноманітні методи оцінювання вразливостей у поєднанні з міжнародними практиками та стандартами управління ІБ [6]. Одним із ключових факторів у контексті ІБ компанії, що потребує оцінювання, є ризики інформаційної безпеки для персоналу під час доступу до ресурсів компанії. З метою надання такої оцінки було вирішено модифікувати відомий технологічний ланцюжок оцінювання ризиків мережевої безпеки [7] і на його основі запропонувати послідовність виконання процесів, що є складовими для оцінювання ризиків ІБ для персоналу під час доступу до ресурсів компанії. Високий рівень ІБ є необхідною умовою для створення та підтримання високої репутації компанії. Належний рівень захисту інформаційних ресурсів підвищує привабливість компанії не тільки для клієнтів, але й для її працівників, що може позитивно вплинути на фінансові результати та подальший розвиток [8–9].

Мета дослідження – вдосконалення підходів до оцінювання ризиків інформаційної безпеки для персоналу компанії під час розмежування доступу до корпоративних інформаційних ресурсів за рахунок розроблення та впровадження модифікованої послідовності процесів, яка враховує специфіку людського чинника і сприяє мінімізації загроз, що виникають через помилки та зловмисні дії персоналу.

1. Аналіз останніх джерел в галузі ІБ в контексті діяльності компанії

Питання взаємозв’язку персоналу та безпеки інформаційних ресурсів компанії розглядали багато українських та закордонних дослідників. Ця проблема охоплювала різні аспекти, включаючи управління персоналом, контроль доступу до інформації та вдосконалення навичок співробітників. Серед українських учених, які досліджували цю тему, варто відзначити Г. Смоквіну, О. Янковську, Ю. Якименко, Т. Мужанову, С. Легомінову, О. Кір’яна, Д. Торяника, Н. Ягнеш, В. Тітову, Ю. Кльоца, В. Волинця, Н. Петляк, М. Огородник та інших.

Питання інформаційної безпеки компанії як процес, що включає визначення потреби в кількості та якості персоналу, його залучення та ефективну розстановку, прогнозування структури, а також оцінювання результатів діяльності й удосконалення професійних знань і навичок, дослідили Г. Смоквіна та О. Янковська [10].

Система управління інформаційною безпекою, яку описали Ю. Якименко, Т. Мужанова та С. Легомінова, представлена як комплекс взаємопов'язаних процесів. Вона охоплює управління персоналом, засобами захисту, ризиками, інцидентами та ресурсами, що дозволяє забезпечити повний цикл кібербезпеки на підприємстві [11]. Важливість освітніх процесів, що спрямовані на підвищення обізнаності персоналу щодо основ інформаційної безпеки, підкреслили О. Кір'ян, Д. Торяник та Н. Ягнеша. Їхні рекомендації включають навчання працівників протидії можливим ризикам у кіберпросторі, що сприяє адаптації персоналу до сучасних вимог інформаційної безпеки [12].

У дослідженні, яке виконали В. Тітова, Ю. Кльоц, В. Волинець, Н. Петляк та М. Огородник, було наголошено на необхідності формування внутрішніх правил і норм, які регламентують поведінку співробітників для забезпечення інформаційної безпеки. Також у роботі описано основні засоби захисту інформації, що є критичними для підвищення рівня безпеки в організації [13].

Серед іноземних дослідників, що розглядали питання взаємозв'язку персоналу та безпеки інформаційних ресурсів компанії, можна виокремити M. Karjalainen, M. Siponen, S. Sarker, K. Khando, S. Gao, S. M. Islam, A. Salman, S. Sharma, M. Warkentin та інших.

У дослідженні, проведеному M. Karjalainen, M. Siponen та S. Sarker, розроблено концептуальні підходи до покращення інформаційної безпеки компанії через визначення основних етапів управління цим процесом. Розроблені етапи можуть значно підвищити ефективність навчання персоналу основам інформаційної безпеки [14].

Дослідження K. Khando, S. Gao, S. Islam та A. Salman зосереджене на вивченні гейміфікації та теоретичних моделей, які використовуються для навчання персоналу основам інформаційної безпеки. Дослідники з'ясували, що ці методи широко використовуються у приватних і державних організаціях, тоді як конструктивістський підхід та методи виявлення порушень здебільшого застосовуються в приватних структурах [15].

S. Sharma та M. Warkentin підтвердили, що рівень організаційної підтримки та прихильності значно впливає на поведінкові наміри персоналу щодо використання інформаційних ресурсів компанії, що є особливо відчутним серед постійних працівників, і забезпечує загальний рівень безпеки [16].

Проаналізувавши актуальні наукові джерела у відкритому доступі, можна дійти висновку, що тема зв'язку персоналу та безпеки інформаційних ресурсів компанії в контексті його оцінювання є актуальною, оскільки викликає широкий інтерес у багатьох вітчизняних і закордонних дослідників.

Проте питання визначення послідовності виконання процесів, що є складниками для оцінювання ризиків інформаційної безпеки для персоналу під час доступу до ресурсів компанії, потребує більш ґрунтовної наукової уваги через перманентне збільшення небезпечності цих ризиків в умовах загострення ситуації з інформаційною безпекою у всьому світі.

2. Технологічна послідовність процесів оцінювання ризиків ІБ для персоналу під час доступу до ресурсів компанії

Інформаційна безпека компанії охоплює інструменти та процеси, які вона використовує для захисту інформації від несанкціонованих дій, тобто попереджає доступ неавторизованих осіб до ділової чи особистої інформації.

Приблизно два десятиліття тому, паралельно з розвитком фундаментальних теорій і методів оцінки та управління ризиками мережевої безпеки, з'явився напрям оцінки та управління ними [17–18]. Хоча ці фундаментальні принципи і методології залишаються невід'ємними, за останнє десятиліття з'явилися значні теоретичні досягнення і практичні моделі. На рис. 1 показано технологічний ланцюжок, що регулює ризики мережевої безпеки [3, 7], який охоплює такі процеси, як 1) збір активів, 2) формування переліку активів, 3) аналіз активів, 4) аналіз інфраструктури, 5) порівняльний аналіз інфраструктури, 6) аналіз та оцінка

ризиків, 7) розробка рекомендацій, 8) впровадження засобів контролю, 9) огляд та повторний аудит.

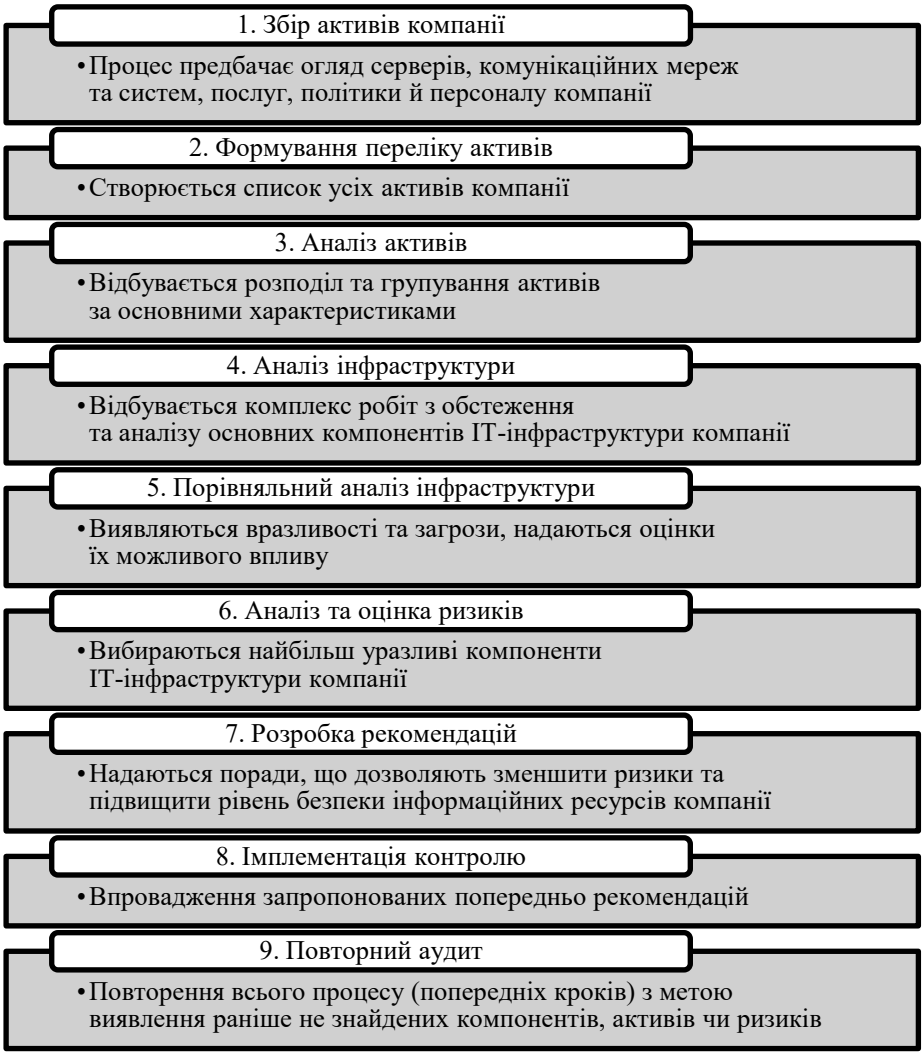

Рис. 1. Технологічний ланцюжок визначення ризиків мережевої безпеки

Збір активів передбачає отримання звітів технічних працівників та кожного окремого працівника компанії, де повинна міститися основна інформація про стан обладнання та характеристики персоналу компанії. Результатом збору активів є формування переліку активів, що відображені в електронному вигляді та зберігається у базі даних. Активи групуються на основі їх стану чи ключових значень, що і є наступним кроком в процесі оцінювання ризиків інформаційної безпеки. Аналіз інфраструктури компанії відбувається шляхом перевірки стану комп'ютерів, серверів та іншого мережевого обладнання. Метою цього аналізу є виявлення найбільш слабких компонентів, до яких зловмисники можуть застосувати шкідливе програмне забезпечення. Порівняльний аналіз інфраструктури компанії проходить перевірку відповідності міжнародним стандартам та вимогам. Під час аналізу потенційних ризиків відбувається оцінка можливого впливу злочинців на інформаційні ресурси компанії. Аналіз дозволяє вибирати адекватні захисні заходи для тих систем і процесів, в яких вони необхідні. Розробка рекомендацій та їх імплементація. Деякі з рекомендацій можуть бути відхилені керівництвом, якщо вважатимуться непотрібними чи дуже затратними до виконання. Результатами рекомендацій є створення контролів. Контроли впроваджуються технічними спеціалістами на місцях, а інформація про це обмежено (частина може зберігатися в таємниці) доноситься до всього іншого персоналу. Останнім кроком процесу оцінювання ризиків ІБ компанії є повторний аудит, що означає виконання всіх кроків знову з метою виявлення

раніше не знайдених компонентів інфраструктури, активів чи потенційних ризиків. Це дозволяє постійно підвищувати рівень безпеки інформаційних ресурсів компанії, бо сам процес оцінювання ризиків інформаційної безпеки є перманентним та безперервним.

Для вирішення задачі оцінювання ризиків інформаційної безпеки для персоналу компанії під час розмежування доступу до корпоративних інформаційних ресурсів пропонується модифікований технологічний ланцюжок процесів оцінювання ризиків інформаційної безпеки для персоналу під час доступу до ресурсів компанії, який складається з дев'яти основних кроків, пояснення яких наведено на рис. 2.

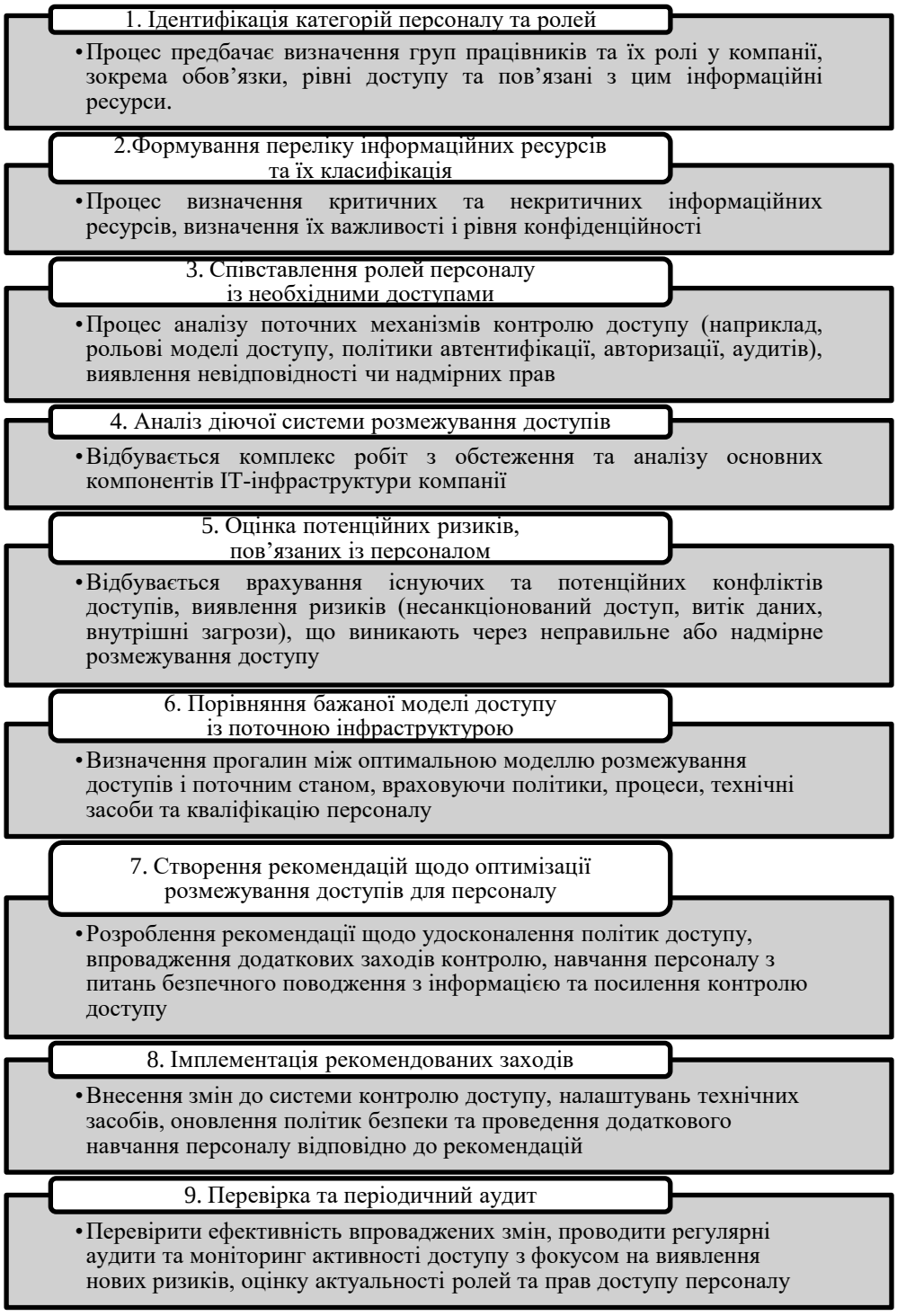

Рис. 2. Модифікований технологічний ланцюжок процесів оцінювання ризиків інформаційної безпеки для персоналу під час доступу до ресурсів компанії

1) Ідентифікація категорій персоналу та ролей. Завдання етапу: визначити, які категорії працівників (адміністратори, технічні фахівці, менеджери, звичайні користувачі, гості тощо) існують у межах компанії; призначити конкретні ролі, що відображають рівень та тип доступу до інформаційних ресурсів:

- аналіз внутрішніх процесів: провести опитування, інтерв'ю або анкетування з метою з'ясування реального функціоналу кожної ролі;
- детальне документування: чітко описати повноваження й обов'язки кожної категорії персоналу, щоб уникнути перетинань та суперечностей;
- регулярний перегляд: періодично переглядати розподіл ролей у зв'язку зі змінами в організаційній структурі чи процесах.

2) Формування переліку інформаційних ресурсів та їх класифікація. Завдання етапу: визначити, якими інформаційними ресурсами (бази даних, електронна пошта, внутрішні сховища, CRM-системи, комерційна таємниця тощо) володіє компанія; провести їх класифікацію за критеріями критичності, конфіденційності й впливу на бізнес-процеси:

- стандартизовані методики класифікації: використовувати міжнародно визнані підходи (iso 27001, nist тощо), щоб систематизувати дані;
- повний облік ресурсів: залучити всі підрозділи компанії, аби жоден ресурс не залишився поза увагою;
- електронні реєстри: створити централізований реєстр (базу даних) зі зручною пошуковою та звітною системами для оперативного доступу та оновлення даних.

3) Співставлення ролей персоналу із необхідними доступами. Завдання етапу: визначити, які ресурси є необхідними для виконання конкретних ролей та завдань у компанії; забезпечити, щоб рівень доступу відповідав посадовим обов'язкам та не перевищував їх:

- аналіз робочих процесів: чітко відстежити, якими системами та документами користується кожна роль у своїй щоденній діяльності;
- принцип мінімальних привілеїв (Least Privilege): надавати кожному співробітнику найменший обсяг доступів, необхідних для виконання роботи;
- політики Role-Based Access Control (RBAC): використовувати рольовий підхід до керування доступом, щоб легко додавати/змінювати або вилучати доступ для груп працівників, а не для кожної особи окремо [19].

4) Аналіз діючої системи розмежування доступів. Завдання етапу: вивчити, яким чином реалізовано надання, перевірку та відкликання доступу до інформаційних ресурсів; зрозуміти сильні сторони та вразливі місця існуючої системи:

- аудит політик та процедур: перевірити поточні інструкції й регламенти, щоби виявити, як вони реалізуються на практиці;
- використання тестових сценаріїв: змоделювати практичні кейси (наприклад, звільнення співробітника, зміну посади чи надання доступу новому відділу), щоб виявити «вузькі місця» в розмежуванні доступу;
- робота з логами та журналами подій: аналізувати журнали аутентифікації, змін паролів, внесення змін до ролей, щоб виявити потенційні порушення або пропуски в безпеці.

5) Оцінка потенційних ризиків, пов'язаних із персоналом. Завдання етапу: виявити, як дії чи бездіяльність працівників можуть загрожувати інформаційним ресурсам (наприклад, фішингові атаки, слабкі паролі, людські помилки, внутрішні зловмисники); оцінити рівень цих ризиків із точки зору ймовірності та впливу:

- проактивні методи оцінки: використовувати опитування та психологічні тести, щоб виявити «зони ризику» в поведінці та знаннях співробітників;
- інструменти для аналізу ризиків: застосувати відомі методології (наприклад, OCTAVE, CORAS, ISO 27005), щоби виміряти й ранжувати загрози;
- систематичне навчання: проводити тренінги з кібергігієни, навчати правил безпечної поведінки та реагування на можливі атаки (фішинг, соціальна інженерія тощо).

6) Порівняння бажаної моделі доступу із поточною інфраструктурою. Завдання етапу: співставити «цільову» модель розмежування доступів із реальною інфраструктурою й політиками безпеки, які діють у компанії; зрозуміти, які зміни необхідні для досягнення бажаного рівня безпеки:

- використання референтних моделей: орієнтуватися на міжнародні стандарти та еталонні системи (COBIT, ITIL, Zero Trust тощо);
- приоритезація змін: визначити, які зони найбільш критичні й потребують негайної уваги, а які можна впроваджувати поетапно;
- оцінка вартості впровадження: поєднати безпекові переваги із загальними бізнес-цілями, щоб уникнути надмірних або неоправданих витрат.

7) Створення рекомендацій щодо оптимізації розмежування доступів для персоналу. Завдання етапу: розробити набір конкретних рекомендацій або план заходів, які покращать існуючу систему доступу з урахуванням реалій компанії; врахувати технічні, організаційні та людські аспекти впровадження:

- комплексний підхід: розглянути не лише технічні рішення (ПЗ, апаратне забезпечення), а й організаційні (процедури, політики, інструкції) і кадрові заходи (навчання, відповідальність);
- гнучкість рекомендацій: формувати пропозиції з урахуванням розміру компанії, наявного бюджету та специфіки галузі;
- залучення керівництва: представити рекомендації мовою бізнес-переваг, щоб отримати підтримку й необхідні ресурси для реалізації.

8) Імплементація рекомендованих заходів. Завдання етапу: перекласти рекомендації у практичні дії: перепроєктувати інфраструктуру, оновити політики доступу, впровадити нові процедури тощо; здійснити контрольоване впровадження з урахуванням можливих ризиків змін:

- покроковий план реалізації: розділити процес на етапи, прописати терміни, відповідальних осіб та очікувані результати;
- пілотне впровадження: випробувати зміни на обмеженій групі (відділі) перед масштабним розгортанням, щоб переконатися в їх коректності та ефективності;
- система індикаторів: підготувати показники (KPI, KRI) для об’єктивної оцінки успішності імплементації.

9) Перевірка та періодичний аудит. Завдання етапу: здійснити моніторинг і періодичний аудит оновленої системи розмежування доступів, щоб оперативно виявляти вразливості; забезпечити безперервний процес удосконалення безпеки:

- регулярні перевірки: проводити планові та позапланові аудити (внутрішні та зовнішні), щоб тримати систему під постійним контролем;
- автоматизовані засоби моніторингу: використовувати інструменти IDS/IPS, системи SIEM, логування та аналіз журналів подій для постійного відстеження підозрілої активності;
- зворотний зв’язок від користувачів: створити канал комунікації, де співробітники зможуть повідомляти про потенційні проблеми або незручності, пов’язані з доступом.

Для вирішення задачі оцінювання ризиків інформаційної безпеки для персоналу компанії під час розмежування доступу до корпоративних інформаційних ресурсів пропонується комплексна модель оцінювання ризиків інформаційної безпеки для персоналу під час розмежування доступу до корпоративних ресурсів (рис. 3), яка враховує специфіку людського чинника і сприяє мінімізації загроз, що виникають через помилки та зловмисні дії персоналу.

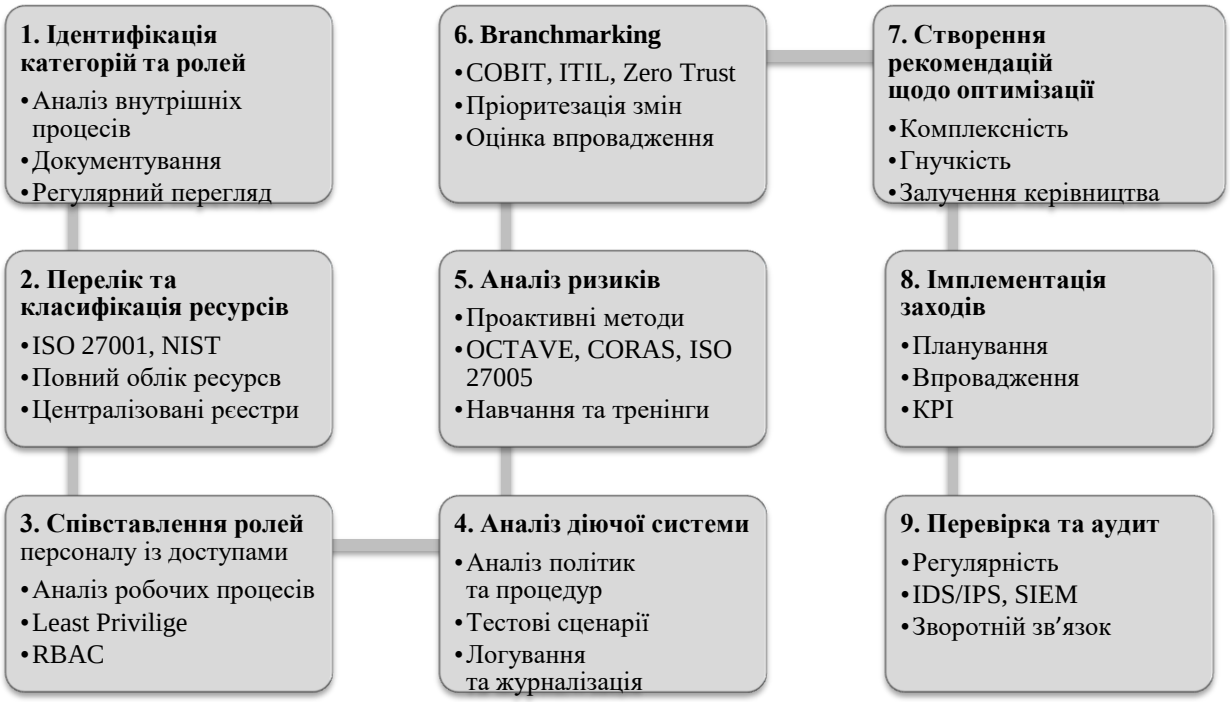

Рис. 3. Комплексна модель оцінювання ризиків інформаційної безпеки для персоналу під час розмежування доступу до корпоративних ресурсів

3. Інформаційна безпека у контексті профілювання персоналу

Інформаційна безпека передбачає всі процеси щодо інформації: її перевірку, модифікацію, записування, будь-яке порушення чи знищення і тісно пов'язана із системами управління ризиками та правовими нормами [18]. Основними принципами інформаційної безпеки та технічного захисту інформації компанії є «тріада CIA» (Confidentiality, Integrity, Availability). Сутністю цих трьох принципів інформаційної безпеки та технічного захисту інформації компанії є:

1. Конфіденційність означає певні заходи, що призначені для запобігання несанкціонованому розголошенню інформації. Метою принципу конфіденційності є збереження особистої інформації, тобто бачити її чи мати до неї доступ можуть тільки ті особи, які нею володіють або потребують її для виконання своїх посадових обов'язків.
2. Принцип цілісності передбачає захист від несанкціонованих змін даних, зокрема додавання, видалення, модифікація тощо, тобто гарантує, що дані є точними й надійними і не змінюються помилково чи зловмисно.
3. Доступність – це захист здатності системи робити дані повністю досяжними для авторизованих користувачів у будь-який час. Іноді через погіршення роботи сервера трапляються випадки відмови від обслуговування, тому мета принципу доступності – зробити технологічну інфраструктуру, програми та дані доступними, коли вони потрібні для робочого процесу або для клієнтів компанії [20–21].

Але, оскільки працівник як актив компанії є унікальним, бо має власний набір навичок та вмінь, переваг і недоліків, то він не може прямо порівнюватись з іншими активами компанії. Сума різноманітних факторів кожного працівника формує його власний профіль [14]. Профілювання надає можливість визначити різницю відповідності профілів працівників до критеріїв компанії та порівнювати їх між собою.

У контексті захисту інформаційних ресурсів компанії користувачів розділяють на групи з різними правами доступу (ці дані також є частиною профілю працівника):

– адміністратори мережі – можуть створювати та управляти політикою інформаційної безпеки, мають дозвіл на зміну глобальних налаштувань мережі;

- технічні працівники (інженери) – проводять регулярне обслуговування IT-інфраструктури компанії (техніки, обладнання, мереж);
- інший персонал – використовують інформаційні ресурси для виконання необхідних завдань, тому мають усі права стандартного користувача (профіль з обмеженим доступом);
- гостьовий профіль – обмежений обліковий запис для покупця чи користувача послуг компанії.

На основі створення цих груп користувачів здійснюється політика розмежування доступу. Весь персонал компанії, що не є адміністраторами чи технічними спеціалістами, зазвичай можуть виконувати всі необхідні операції з інформаційними ресурсами, крім таких, як: завантаження робочих файлів; створення власних груп користувачів чи зміна вже наявних; зміна налаштувань серверів та мережі; підключення нової IT-інфраструктури; самостійне встановлення програмного забезпечення; підключення зовнішнього обладнання.

Більшість моделей розмежування прав доступу до інформаційних ресурсів побудовано на основі методу парольної автентифікації. Вони не вимагають залучення великого обсягу апаратних та програмних компонентів, але часто можуть мати сумнівну надійність. Відомі також методи автентифікації, які передбачають використання інших засобів, котрі надають кращий рівень захисту, ніж автентифікація за допомогою паролю [15].

Питання хешування має прямий зв’язок із процесом автентифікації користувачів, оскільки за його допомогою в деяких моделях розмежування прав доступу відбувається одночасна автентифікація користувача та самого пристрою (робочої станції) перед наданням доступу до необхідного інформаційного ресурсу компанії.

Висновки

Розглянуто взаємозв’язок між персоналом компанії та рівнем захищеності її інформаційних ресурсів, проаналізовано існуючі підходи до оцінювання ризиків інформаційної безпеки. Особливу увагу приділено комплексу заходів, спрямованих на формування політики розмежування доступу, що враховує специфіку людського чинника.

Досягнуто мети, яка передбачала вдосконалення підходів до оцінювання ризиків інформаційної безпеки для персоналу компанії під час розмежування доступу до корпоративних інформаційних ресурсів за рахунок розроблення та впровадження модифікованої послідовності процесів, що мінімізує загрози, пов’язані з помилками та зловмисними діями працівників. Запропоновано технологічний ланцюжок, який містить дев’ять послідовних етапів оцінки ризиків, серед яких виокремлено ідентифікацію категорій персоналу й ролей, формування переліку інформаційних ресурсів та їх класифікацію, оцінку потенційних ризиків тощо.

Запропоновано комплексну модель оцінювання ризиків інформаційної безпеки для персоналу, що враховує унікальні характеристики працівників і дає змогу деталізувати політику доступу відповідно до профілю кожного користувача. Особливу увагу приділено профілюванню персоналу, методам автентифікації та механізмам перевірки робочих станцій. Виокремлено практичні рекомендації щодо організації періодичного аудиту, навчання персоналу, впровадження проактивних методів аналізу ризиків та гейміфікованих підходів, що підсилюють рівень захисту.

Отже, використання описаного підходу дає можливість комплексно оцінити й контролювати ризики інформаційної безпеки, пов’язані з людським чинником, і сприяє підвищенню загального рівня захисту корпоративних ресурсів та оптимізації процесів розмежування доступу в компанії.

Список літератури:

1. N. Kaloudi and J. Li. AST-SafeSec: Adaptive Stress Testing for Safety and Security Co-Analysis of Cyber-Physical Systems // IEEE Transactions on Information Forensics and Security. 2023. Vol. 18. pp. 5567–5579. doi: 10.1109/TIFS.2023.3309160.

2. «Ukraine - Data Protection Overview.» DataGuidance, 12 Nov. 2024, www.dataguidance.com/notes/ukraine-data-protection-overview.

3. Korobeinikova T., Tachenko I., Romanyuk O., Romanyuk S., Stakhov O. and Reyda O.. Assessing Network Security Risks: a Technological Chain Perspective // 14th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2024, pp. 565–570, doi: 10.1109/ACIT62333.2024.10712586.

4. Міщук Є., Іванов Р. (2024). Управління персоналом для забезпечення кадрової безпеки підприємства // Успіхи і досягнення у науці, 2024. № 6.

5. Корченко А. та ін. Метод формування параметрів та оцінювання загроз у соціотехнічних системах // Information Technology: Computer Science, Software Engineering and Cyber Security. 2023. № 2. С. 3–11. Режим доступу: https://doi.org/10.32782/IT/2023-2-1.

6. Kurii Y. Opirskyy I. ISO 27001: аналіз змін та особливості відповідності новій версії стандарту // Електронне фахове наукове видання Кібербезпека: освіта, наука, техніка. 2023. 3(19). С. 46–55.

7. Korobeinikova T., Tachenko I., Chekhmestruk R., Mykhaylov P., Romanyuk O. and Romanyuk S. A General Method of Risk Estimation // 13th International Conference on Advanced Computer Information Technologies (ACIT). Wrocław, Poland, 2023, pp. 410–413. doi: 10.1109/ACIT58437.2023.10275626.

8. Воронкова В. Г., Нікітенко В. О. Цифрова трансформація промислового підприємства : наук.-метод. посіб. Запоріжжя : ЗНУ, 2023. 158 с.

9. Мазник Л. В., Драган О. І. Інформаційна безпека організації як фактор посилення бренду роботодавця // Київський економічний науковий журнал. 2023. № 1. С. 39–44. Режим доступу: https://doi.org/10.32782/2786-765X/2023-1-5.

10. Смоквіна Г., Янковська О. Кадрова безпека промислових підприємств: сутність, складові та заходи мінімізації загроз // Економічний журнал Одеського політехнічного університету. 2019. Вип. 7. № 1. С. 38–45. Режим доступу: https://doi.org/10.5281/zenodo.3402729.

11. Якименко Ю., Мужанова Т., Легомінова С. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FireEye // Кібербезпека: освіта, наука, техніка. 2021. Вип. 4. № 12. С. 36–50. Режим доступу: https://doi.org/10.28925/2663-4023.2021.12.3650.

12. Кір'ян О., Торяник Д., Ягнеша Н. Кадрова складова інформаційної безпеки підприємства // Адаптивне управління: теорія і практика. Сер. Економіка. 2024. Вип. 18. № 36. Режим доступу: https://doi.org/10.33296/2707-0654-18(36)-12.

13. Тітова В. та ін. Розроблення політики інформаційної безпеки приватного підприємства // Measuring and computing devices in technological processes. 2024. № 3. С. 79–83. Режим доступу: https://doi.org/10.31891/2219-9365-2024-79-10.

14. Karjalainen M., Siponen M., Sarker S. Toward a stage theory of the development of employees' information security behavior // Computers & Security. 2020. Vol. 93. P. 1–18. Режим доступу: https://doi.org/10.1016/j.cose.2020.101782.

15. Khando K. et al. Enhancing employees information security awareness in private and public organisations: A systematic literature review // Computers & Security. 2021. Vol. 106. P. 1–22. Режим доступу: https://doi.org/10.1016/j.cose.2021.102267.

16. Sharma S., Warkentin M. Do I really belong?: Impact of employment status on information security policy compliance // Computers & Security. 2019. Vol. 87. Режим доступу: https://doi.org/10.1016/j.cose.2018.09.005.

17. ISO 27001 Requirements – Information Security Management // Sprinto, 2021. URL: https://sprinto.com/blog/iso-27001-requirements/.

18. "ISO/IEC 27701:2019." ISO, 17 Oct. 2022, www.iso.org/standard/71670.html.

19. Ямнич А. Б. Модель контролю доступу персоналу до інформаційних ресурсів підприємств на основі RBAC та технології BLOCKCHAIN / А.Б. Ямнич, Т.І. Коробейнікова // Вісник Хмельницького нац. ун-ту. 2024. Т. 343, №6(1). С. 380–386.

20. Imperva. Information Security: The Ultimate Guide. Режим доступу: https://www.imperva.com/learn/data-security/information-security-infosec/

21. Секель А. Цілі інформаційної безпеки та їх значення. Режим доступу: https://www.dqsglobal.com/uk-ua/navchajtesya/blog/cili-informacijnoyi-bezpeki-ta-yih-znachennya.

Надійшла до редколегії 10.10.2024

Відомості про авторів:

Коробейнікова Тетяна Іванівна – канд. техн. наук, доцент, Національний університет «Львівська політехніка», доцент кафедри безпеки інформаційних технологій; Україна; e-mail: tetianakorobeinikova@gmail.com; ORCID: https://orcid.org/0000-0003-2487-8742

Ямнич Андрій Богданович – аспірант кафедри безпеки інформаційних технологій; Національний університет «Львівська політехніка», Україна; e-mail: andrii.b.yamnych@lpnu.ua; ORCID: https://orcid.org/0009-0005-7226-1896