УДК 65.012.32(045)+004.56.5(043.2)

ВИКОРИСТАННЯ ЛОГІКО-КОГНІТИВНИХ ПІДХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ АВТОМАТИЧНОМУ ФОРМУВАННІ ЗАМОВЛЕНЬ НА ПОЛІГРАФІЧНИХ ПІДПРИЄМСТВАХ

П. І. Шепіта, Л. Л. Тупичак

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Проаналізовано тематику наукових праць з впровадження сучасних технологій та систем автоматизованого управління підприємством, його ресурсами та технічними засобами і показано недостатню повноту досліджень щодо особливостей комплексного підходу при проектуванні та розгортанні інноваційних засобів супроводу виробничого замовлення. На основі визначених чинників функціонування підприємства в новітніх умовах четвертої індустріальної революції обумовлено напрямки формування стратегій впровадження елементів Індустрії 4.0 в сучасні поліграфічні підприємства, а також системи захисту інформації при електронному документообігові.

Розглянуто механізми для вирішення завдань управління інформаційними ризиками в складних системах управління поліграфічними підприємствами в умовах невизначеності та при виникненні взаємного впливу елементів системи управління один на одного. Обґрунтовано необхідність використання вебпорталу для формування поліграфічних замовлень, визначено основні компоненти та описано рівні доступу до них.

Для підвищення ефективності рівня інформаційної безпеки системи інтелектуального управління підприємством застосовано один із логіко-когнітивних напрямків – нечітку логіко-когнітивну модель, яка полягає у поєднанні наведених відомостей про зміст загроз, вразливостей системи та засобів захисту між собою. Запропоновані підходи дозволили розглянути вплив потенційних атак на основні сервіси інформаційної безпеки. В процесі роботи обґрунтовано засади захисту інформації в незалежних від людини системах при автоматизованому опрацюванні замовлень на поліграфічних підприємствах, в основу яких покладено логіко-когнітивну методику оцінювання якості мінімізації ризиків втрати або модифікації інформації та незаконного заволодіння даними.

Ключові слова: *інтелектуальна система управління, вебпортал, замовлення, нечітка логіко-когнітивна модель, захист інформації.*

Постановка проблеми. Автоматизація та захист інформації на поліграфічних підприємствах є досить складним та тривалим процесом, який вдосконалюється впродовж десятиліть з моменту появи перших елементів автоматизації для системного поліпшення якості виготовленої продукції, прискорення її виготовлення та

зниження затрат на виробництво, нарощення виробничих потужностей. На сучасному етапі розвитку інформаційних технологій автоматизована система управління під впливом четвертої промислової революції переходить у розряд інтелектуальної системи, яка передбачає автономну роботу без участі людини. У межах зазначених проєктів створюється велика кількість великомасштабних розподілених систем, які часто не мають аналогів як за своєю складністю, з одного боку, так і за розмірами потенційних загроз, що виникають у разі їх відмови або некоректної роботи, з іншого боку. Таким чином, проблема забезпечення інформаційної безпеки та управління ризиками складних систем на сьогодні стає як ніколи актуальною. Причому це стосується не лише активного впровадження наявних методів та засобів з управління ризиками, а й їх удосконалення і розвитку нових підходів для вирішення зазначених проблем з використанням логіко-когнітивних підходів.

Аналіз останніх досліджень та публікацій. Виконані дослідження з цієї тематики присвячені захисту інформації при електронному документообігу на поліграфічних підприємствах та у видавництвах [1, 2]. Однак при проєктуванні інтелектуального управління для поліграфічних підприємств, яке розглядається у публікаціях [3, 4], необхідно враховувати безпеку інформаційної системи, що працює в автоматичному режимі опрацювання замовлень. При звичному документообігу достатньо забезпечити захист, описаний у публікації [5]. Проте інтелектуальна система, яка взаємодіє із замовником безпосередньо через вебпортал, піддається впливу зовнішніх факторів, для запобігання яким виникає потреба ґрунтовного дослідження.

Підхід до вирішення поставленого завдання, коли конкретний вид функцій локального ризику невідомий, вперше був намічений, хоч і трохи в іншій постановці, у статті [6], а найповніше викладений у монографіях [7, 8].

У працях [9–12] описано процес побудови системи захисту інформації та кібербезпеки з використанням глибокого та машинного навчання відповідно до системного і когнітивного методу. Але оскільки кількість замовлень, що отримує поліграфічне підприємство за одиницю часу порівняно, невелика, то застосовувати складний апарат машинного навчання не є доцільним.

Мета статті – формалізоване відображення механізмів, необхідних для вирішення завдань управління інформаційними ризиками в складних системах управління поліграфічними підприємствами в умовах невизначеності та при виникненні взаємного впливу елементів системи управління один на одного.

Виклад основного матеріалу дослідження. На базі проведених досліджень автоматизованих систем управління поліграфічними підприємствами та засобів оперативної поліграфії, а також інтернет-сервісів побудовано модель формування замовлення, в основі якої лежить сучасний кросплатформний інтернет-портал надання поліграфічних послуг з багатопрофільним гнучким інтерфейсом та можливостями динамічного відображення даних та моніторингу, наявних у системах диспетчеризації та управління поліграфічними процесами [13]. При надходженні замовлення потрапляє в базу системи керування, де опрацьовується за своїми складовими, а саме: колірністю, форматом, матеріалом, на якому потрібно

його виготовити, та іншими, пов'язаними з технологічними процесами, що будуть задіяні при виготовленні замовлення та його кінцевому оформленні у готову продукцію. В такому випадку замовлення проходить три основні етапи, представлені на рис. 1. Замовник (користувач інформаційної онлайн-системи) завантажує матеріали, якщо такі наявні, або описує, як він бачить продукт в особистому кабінеті інтернет-ресурсу підприємства.

Рис. 1. Етапи проходження замовлення для формування робочого завдання

Для проєктування такої системи запропоновану онлайн-платформу умовно розділено на дві частини: зовнішню – користувацьку частину, де концентруються кабінети замовників та гостьові сторінки, та внутрішню (інтелектуально-адміністративну), яка функціонує переважно на підприємстві та пов'язана із зовнішньою частиною для оптимізації, пришвидшення та якісного виконання процесів друку, а також для реалізації можливості зовнішнього адміністрування та оптимізації виробничих процесів.

Користувацька частина являє собою онлайн-платформу для реалізації поліграфічної продукції, де формується пропозиція, вимоги та ведеться документообіг і спілкування з клієнтами. Друга частина наповнюється профілями користувачів (працівники підприємства, динамічне відтворення моніторингових даних, підтримка документообігу та інтелектуального управління) [13, 14].

Для функціонування складових платформи введено базу даних адміністрування основних інформаційних потоків платформи. Цей етап полягає в розробці таблиць та зв'язків між ними, забезпеченні зчитування та запису інформації в базу і сортуванні та систематизації. Для реалізації цього пункту прийнято рішення розширити та доповнити наявну корпоративну базу підприємства, а також забезпечити резервне дублювання даних [15].

Останнім етапом є забезпечення працездатності системи та взаємний обмін інформацією між всіма компонентами системи [16]. Для ефективного обігу основних відомостей прийнято рішення про їх категоризацію за профілями користувачів та рівнями складності обчислювальних операцій для системи.

Розроблено схему онлайн-платформи (рис. 2), яка відображає інформаційні потоки між суб'єктами виробничого процесу та елементами інтелектуальної системи управління. Одним із основних блоків є друкарських цех, який містить парк машин із системами керування, засобами контролю якості і моніторингу, а також

додаткові пристрої та логістику матеріалів зі складу. Згідно з цим у базу даних вносяться зміни про товарообіг, готовність замовлень та стадії їх виконання. Окрім цього, протоколювання, звіти та важливі частини документообігу вносяться в базу даних у режимі реального часу. Усі відомості засобами управління базою даних друкарського цеху вносяться у відповідні таблиці для подальшого використання. Інформація з бази даних відображається у відповідних розділах онлайн-платформи. Доступ до інформації мають користувачі з відповідним рівнем доступу [17–19].

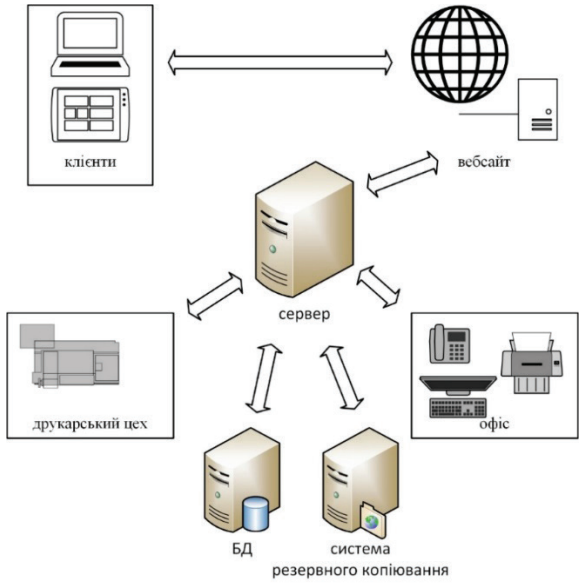

Рис. 2. Інформаційна модель онлайн-системи

З метою забезпечення швидкого обміну даними та стабільного з'єднання з системою пристрої, які працюють в офісі, використовують для передання даних у локальну мережу. Опрацьована інформація з ПК офісу потрапляє в систему, а також дублюється в базі даних. Клієнти, які входять в систему, отримують доступ до зовнішньої частини (сайту) для оформлення замовлень та відслідковування їхнього виконання. Ця функція реалізується через особистий кабінет замовника [20–23].

Адміністративна частина платформи забезпечує комунікацію між працівниками, системою управління та клієнтом (замовником) й дозволяє генерувати теги для формування параметричного опису виконання замовлення [14]. Оскільки в системі знаходиться велика кількість важливих виробничих та корпоративних даних, запропоновано дублювання їх на резервний сервер.

Таким чином, обумовлені етапи розробки онлайн-платформи й конструювання адміністративної частини динамічного вебсервісу відображення даних моніторингу та відслідковування етапів виконання замовлення локалізовані у вигляді базових модулів проєкту корпоративної вебплатформи для якісного та оперативного виконання індивідуального малотиражного замовлення, а також замовлень великих масштабів [24].

На основі обґрунтування необхідності використання онлайн-сервісу для представлення поліграфічної продукції та побудови низки взаємодій користувачів різних профілів виконано проєктування моделі формування замовлення (рис. 3), центральним елементом якої виступає вебінтерфейс користувача, що взаємодіє із замовником, працівником та керівником.

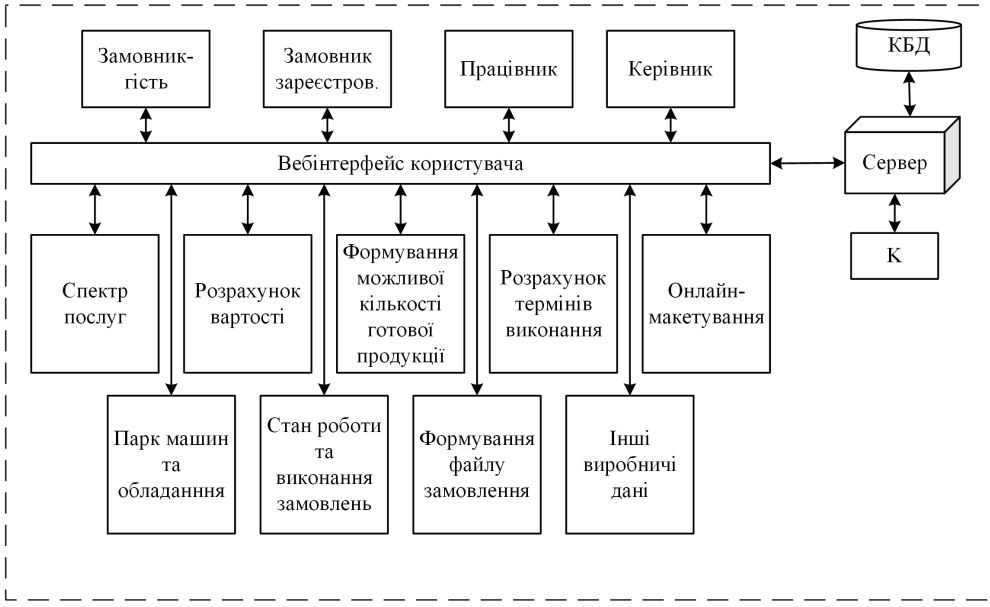

Рис. 3. Модель формування замовлення

Профілювання користувачів дозволяє надавати різні права та можливості залежно від прав доступу, активація таких функцій зменшує навантаження та серверні ресурси підприємства. З цією метою в модель введено чотири основні категорії користувачів, які мають доступ до модулів онлайн-платформи. Замовник-гість розташований у цій ієрархії користувачів на нижньому рівні, оскільки має найменше прав доступу, бо тільки потрапив на платформу для створення першого замовлення. У зв'язку з цим він поки що не має можливості відстеження замовлення в реальному часі, а також прямого зв'язку з особистим консультантом, на відміну від замовника (зареєстрованого користувача). Створення особистого кабінету надає можливість на вебінтерфейсі відкрити функцію відстеження поетапного проходження замовлення стадіями виробництва поліграфічного підприємства, а також передбачає можливість відстеження готової продукції, яка упакована та направлена до клієнта. Особистий кабінет надає можливості для онлайн-макетування, обрання матеріалів та типу продукції для формування виробничого замовлення. В режимі реального часу відбувається розрахунок вартості замовлення, виходячи з обраних параметрів, а також залежно від завантаженості виробництва та наявних на складі сировини матеріалів проводиться розрахунок термінів виготовлення замовлення. Замовник за бажанням надає згоду для отримання сповіщень про

стадії проходження замовлення, що дозволяє збільшити інформування клієнтів та зменшити навантаження на операторів-менеджерів, які відповідають за зворотній зв'язок з клієнтами [25–28].

Профіль працівника дозволяє кваліфікованому персоналу поліграфічного підприємства, використовуючи засоби мережі Інтернет, під'єднатись спільно до системи управління підприємством, щоб проводити вимірювання та налагодження пристроїв та агрегатів робочого процесу віддалено. Однак важливою складовою, властивою профілю працівника, є моніторинг обладнання та ресурсів підприємства. Оскільки кваліфікований персонал в розрізі підприємства також вміщує й адміністративні блоки, що лише дотично належать до виробничого цеху (наприклад, бухгалтерія, відділ кадрів, склад та ін.), передбачено ще й внутрішнє профілювання працівників, яке корелює з їхніми функціями на поліграфічному підприємстві [29–31].

Профіль керівника виділено в окремий блок, що пов'язано з типом профілю, оскільки він має аналітичну мету – дозволяє переглядати статистику замовлень, кількість виконаних замовлень, кількість замовлень, що перебувають у роботі, та різні адміністративні параметри, яких потребує керівник підприємства.

Комунікація всіх рівнів користувачів відбувається через вебінтерфейс користувача, який пов'язаний через сервер підприємства із корпоративною базою даних. Така організація дозволяє об'єднувати різні параметри виробничого циклу, адміністративні протоколи. Блок «спектр послуг» засвідчує типи продукції, які може виготовляти підприємство, використовуючи обладнання, перелік якого розташований в блоці «парк машин та обладнання». Доступ до переліку обладнання мають профілі користувачів «працівник» та «керівник». Наявність такого сегмента в онлайн-платформі дозволяє відстежувати стан обладнання і надає можливість його налаштування та віддаленого переналагодження [32].

Розрахунок вартості слугує для клієнта інформаційним джерелом про вартість готового продукту за його вибором, а орієнтовна дата виготовлення реалізується в блоці «розрахунок термінів виконання». Важливим етапом роботи вебсервісу є формування замовлення та завантаження макета. Цей етап запропоновано реалізовувати двома шляхами: на першому завантажується готовий макет через вікно в особистому кабінеті користувача; другий передбачає створення макета онлайн-засобами макетування в особистому кабінеті. Для передання даних, які спеціалізуються та структуруються на онлайн-платформі, в модель процесу формування замовлення введено файл-контейнер К, який переносить дані на наступний етап проходження замовлення [32].

На основі викладеного побудовано схему узгодженості доступу користувачів до основних блоків онлайн-платформи (рис. 4).

Вебінтерфейс отримує дані про користувачів у вигляді множини, яка розміщена у файлі автентифікації. Розподіл за блоками відбувається згідно із присвоєною множиною, властивою індивідуально для кожного. Користувачі, ідентифікатор яких вміщено у множину, можуть використовувати всі властивості блоку, які отримуються інтерфейсом через шину даних [32–34].

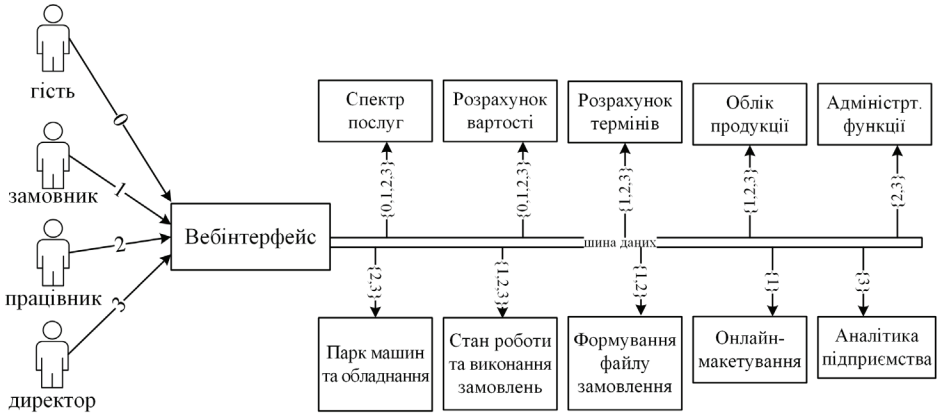

Рис. 4. Блок-схема узгодженості доступу до блоків онлайн-системи

В результаті побудови моделі формування замовлення обумовлено важливі етапи проєктування онлайн-платформи для поліграфічного підприємства, визначено передумови для інтеграції вебплатформи у виробництво як інтелектуального сервісу системи управління підприємством.

На основі обумовленої стратегії роботи вебпорталу поліграфічного підприємства для автоматичного формування замовлень виявлено необхідність проєктування керування інформаційними ризиками інтелектуальної системи управління з використанням логіко-когнітивних підходів захисту інформації [35–37].

Для нашої системи інтелектуального управління із комунікаційним вебпорталом визначаємо модель управління інформаційними ризиками (1):

$$\left\langle SK, X, S = \{s_i\}, \{\rho_i(\bullet)\}\rho(\bullet), i \in N \right\rangle. \tag{1}$$

Будемо вважати, що в рамках загальної моделі метою суб'єкта *SK* є використання доступних йому ресурсів *X* і проведення їх розподілу між елементами системи *S,* що дозволяє досягти максимально можливого зниження інтегрального ризику ρ (*x*). Функція локального ризику $\rho_i(\cdot)$ зі свого боку складається з множини суворо монотонних функцій, що спадають за всіма аргументами.

Запишемо множину (2) допустимого розподілу ресурсу *X* між елементами системи *S* та системи управління *SK:*

$$\Omega(X) = \left\{ (x_1, \ldots, x_n) \notin R^n : x_i \geq 0, i \notin N, \sum_{i=1}^{n} x_i \leq X \right\}. \tag{2}$$

Тоді формалізуємо мету *SK* до вигляду (3):

$$ics_{x \in \Omega(X)} \rho(\Omega) = ics_{x \in \Omega(X)} \rho\left(\rho_1(\Omega), \ldots, \rho_n(\Omega)\right). \tag{3}$$

Але оскільки нам невідомо, який тип функції локального ризику використовувати, стає очевидною необхідність переходу від глобального завдання мінімізації інтегрального ризику до локального, метою якого є зниження максимуму локальних ризиків $\rho_i(\cdot)$, $i \in N$.

Очевидно, що для вирішення завдання, описаного виразом (3), виникає необхідність використання експертного підходу. Проте такий спосіб мінімізації ризиків є досить умовним, оскільки вся відповідальність на совісті людини-експерта. У зв'язку з цим прийнято рішення побудувати незалежну від людини систему захисту інформації при автоматизованому опрацюванні замовлень на поліграфічних підприємствах. В основу такої системи покладено логіко-когнітивну методику оцінювання якості мінімізації ризиків втрати або модифікації інформації та незаконного заволодіння даними [38, 39].

Виходячи із режимів доступу, описаних у блок-схемі рис. 4, видно, що найуразливішими місцями в системі управління, в яку інтегровано вебпортал, є блоки, доступ до яких має найбільша кількість користувачів.

Використовуючи засади комплексної інформаційної безпеки для інтелектуальної системи управління поліграфічним підприємством, необхідно забезпечити дотримання наступних політик, а саме: перша фінансова політика розширення, розвитку та підтримки в актуалізованому стані корпоративної мережі поліграфічного підприємства; друга політика забезпечується рівнем організації розгортання та супроводу корпоративних ресурсів підприємства, корпоративної бази даних та знань; третя політика належить до кадрового складу та потребує досвідчених системних адміністраторів. В умовах інформаційних загроз слід приділити увагу політиці програмного забезпечення захисту інформації та оновленню застарілого обладнання загалом, яке сьогодні є одним із критичних факторів при оцінці працездатності та захищеності корпоративних ресурсів [39–41].

На основі обумовлених політик захисту інформації при автоматичному замовленні виділимо основні заходи забезпечення захисту корпоративних даних у мережі інтелектуальної системи управління: Z_1 – організація процедури зберігання документів; Z_2 – розробка процедури оперативного реагування на інциденти; Z_3 – адміністративні та технічні засоби контролю за роботою користувачів; Z_4 – використання лише сертифікованого та ліцензійного програмного забезпечення для розробки програмного продукту та його супроводу; Z_5 – розмежування доступу до елементів системи управління; Z_6 – технічна підтримка апаратних ресурсів; Z_7 – створення локальних і хмарних резервних копій системи та її даних; Z_8 – навчання штатних працівників-операторів основам інформаційної безпеки; Z_9 – розробка нормативної документації із заходів інформаційної безпеки; Z_{10} – організація аналітично-контролюючої роботи; Z_{11} – розгортання при впровадженні системи управління з вебпорталом оптимальних корпоративних мереж; Z_{12} – резервування засобів та каналів комунікації; Z_{13} – використання криптографічних засобів захисту інформації; Z_{14} – впровадження засобів розподіленого доступу до інформаційних ресурсів; Z_{15} – використання технології міжмережевого екранування; Z_{16} – інтегрування засобів аналізу захищеності даних; Z_{17} – інтегрування засобів виявлення кібератак; Z_{18} – використання концепції антивірусного захисту при проєктуванні системи управління; Z_{19} – розроблення протоколу відновлення системи управління після атак та аварійного режиму; Z_{20} – використання засобів контентного аналізу; Z_{21} – обов'язкова наявність системи резервного

електропостачання. Наведені засоби захисту інформації зводимо у множину засобів протидії кібератакам $Z=\{Z_i\}$ [40, 42].

З метою оцінки рівня інформаційної безпеки системи інтелектуального управління підприємством застосуємо один із логіко-когнітивних напрямків – нечітку логіко-когнітивну модель, яка полягає у поєднанні наведених відомостей про зміст загроз, вразливостей системи та засобів захисту між собою. Таке поєднання дозволило розглянути вплив потенційних атак на основні сервіси інформаційної безпеки. При цьому на нижньому рівні ієрархії *G* розташовуються засоби та механізми захисту *Z*, дії яких зменшують ймовірність виникнення загроз *ZG* та послаблюють рівень вразливостей *VZ*, розташованих на рівень вище, а також, загрози та вразливості, що зі свого боку визначають можливість виникнення атак *A*, які негативно впливають на сервіси безпеки *SRB*.

Як найбільш значущі для поліграфічного підприємства оберемо наступні парадигми безпеки: конфіденційність, цілісність і доступність. Ці множини визначають інтегральний показник комплексної інформаційної безпеки поліграфічного підприємства *PP* та впливають на рейтингові показники, репутацію, матеріально-технічний стан, фінансову стійкість, якість надання поліграфічних послуг тощо [40]. У кожному компоненті інтелектуальної системи управління виділяємо інформаційні активи та виконуємо їх ранжування за ступенем значущості відповідно до ймовірності кібератак на кожен актив. З множин *ZG* і *VZ* потрібно відібрати загрози та вразливості, характерні для кожного з наявних активів. Після чого складається перелік засобів інформаційної безпеки та їх впливу на сформульовані загрози. При цьому всі оцінки задаються за допомогою лінгвістичної змінної «Рівень фактора» з терм-множиною *TS*={Низький (*L*), Нижчий за середній (*ML*), Середній (*M*), Вище середнього (*AA*), Високий (*H*)}. Обчислення значень факторів проводиться за такими формулами:

$$\overline{VZ}_j^{mn} = VZ_j^{mn} \cdot \prod_i Inv\left(Z_i^{mn}\right)^{r_i^{mn}}, \tag{4}$$

де $Inv(F) = 1 - \mu_F$ – інверсія довільного нечіткого числа *F*; $\overline{VZ}_j^{mn}$ – залишковий (після застосування засобів захисту) рівень *j*-ї вразливості *m*-го активу щодо *n*-ї небезпеки; VZ_j^{mn} – вихідний (до застосування засобів захисту) рівень *j*-й уразливості *m*-го активу щодо *n*-ї загрози; Z_j^{mn} – рівень *i*-ї захисної дії щодо *n*-ї загрози *m*-му активу; r_i^{mn} – ваговий коефіцієнт, що вказує значущість *i*-го захисного рівня зниження *n*-ї загрози *m*-у активу;

$$\overline{VZ}_j^{mn} = Inv\left[\prod_j Inv\left(\overline{VZ}_j^{mn}\right)^{s_j^{mn}}\right], \tag{5}$$

де $\overline{VZ}^{mn}$ – інтегральний рівень вразливості *m*-го активу стосовно *n*-ї загрози; s_j^{mn} – ваговий коефіцієнт, що відображає «вклад» $\overline{VZ}_j^{mn}$ в $\overline{VZ}^{mn}$;

$$\overline{ZG}_n^m = ZG_n^m \cdot \prod_i Inv\left(Z_i^{mn}\right)^{v_i^{mn}}, \tag{6}$$

де ZG_n^m – залишкова ймовірність існування загрози ZG_n для *m*-го активу після застосування сукупності засобів захисту Z_j^{mn}; ZG_n^m – вихідна ймовірність існування

загрози ZG_n m-му активу; v_i^{mn} – ваговий коефіцієнт, що відображає вплив елемента захисту Z_i^{mn} для зменшення загрози ZG_n^m.

Відзначимо, що всі описані параметри в цілому можуть бути функціями часу t, тому при проведенні динамічних розрахунків слід задавати їх початкові значення при часі $t = 0$ і враховувати крок зміщення за часом [43, 44].

Реалізація n-ї загрози для m-го активу $\overline{ZG}_n^m$ з використанням тих вразливостей, що залишилися $\overline{VZ}^{mn}$, викликає атаку A_n^m. Знаходимо оціночну ймовірність виникнення кібератаки з використанням формули (7):

$$A_n^m = ZG_n^m \cdot \overline{VZ}^{mn}. \tag{7}$$

Якщо ця оціночна ймовірність відмінна від нуля, то ми отримуємо, незважаючи на вжиті захисні заходи, що в деякий момент часу t^{mn} кібератака A_n^m все ж виникла, тому необхідно вжити заходів Z_j^{mn} з метою зниження рівня порушень безпеки інформаційного простору поліграфічного підприємства.

Отриманий оціночний коефіцієнт дозволяє побудувати інтерактивну систему захисту конфіденційних даних підприємства, яка з використанням аналітичного апарату інтелектуальної системи управління дозволить відпрацювати можливі джерела загроз, а також побудувати з використанням нечітких множин когнітивної логіки та штучних нейронних мереж ядро «захисника» системи управління для реалізації автоматичного формування замовлень через описаний вебпортал, індексуючи рівень небезпеки від користувачів відповідно до їхніх прав доступу.

Висновки. Розвиток інформаційних технологій інтенсивно впливає на автоматизовані процеси виготовлення замовлення, зниження затрат на виробництво, нарощення виробничих потужностей та якість виготовленої продукції.

У дослідженні сконцентровано увагу на логіко-когнітивній методиці оцінювання якості мінімізації ризиків втрати інформації та незаконного заволодіння даними. Окрім вищенаведеного, побудовано модель формування замовлення, в основі якої лежить сучасний кросплатформний інтернет-портал надання поліграфічних послуг з багатопрофільним гнучким інтерфейсом та можливостями динамічного відображення даних та моніторингу, наявних у системах диспетчеризації та управління поліграфічними процесами.

В результаті дослідження виконано аналіз основних показників захисту інформаційних потоків поліграфічного виробництва на основі сформульованих парадигм організації вебпорталу поліграфічного підприємства. Аналіз чинників впливу загроз на систему інтелектуального управління дав можливість отримати оціночний коефіцієнт стійкості інтелектуальної системи управління поліграфічним підприємством до зовнішніх загроз інформаційній безпеці.

Отже, використання спеціалізованих систем автоматизації і захисту дозволяє підвищити оперативність виробничої діяльності підприємства в цілому під час процесу передання замовлення у виробництво, формування й перерахунку плану виробництва, реалізації робочих процесів диспетчеризації, формування системи звітності та роботи з готовою продукцією.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дурняк Б. В., Сабат В. І., Шведова Л. Є. Управління повноваженнями в системах захисту інформації : монографія. Львів : УАД, 2016. 148 с.
2. Сабат В. І., Мацюк В. В., Мусійовська М. М., Каневська Н. І. Розроблення системи управління доступом до документів в АСДО для поліграфічних видавництв. *Наукові записки [Української академії друкарства]*. 2020. № 2 (60). С. 68–74.
3. Шепіта П. І. Інформаційна модель динамічного вебсервісу інтелектуальної системи управління. *Комп'ютерні технології друкарства*. 2019. № 2 (42). С. 73–80.
4. Шепіта П. І. Синтез інформаційної моделі інтелектуального управління поліграфічним виробництвом на основі штучних нейронних мереж. *Моделювання та інформаційні технології.* 2018. № 85. С. 192–196.
5. Сабат В. І., Шепіта П. І. Функціональна модель системи захисту автоматизованої системи документообігу. *Моделювання та інформаційні технології.* 2018. № 84. С. 190–195.
6. Калашников А. О. Управление информационными рисками с использованием арбитражных схем. *Системы управления и информационные технологии.* 2004. № 4 (16). С. 57–61.
7. Калашников А. О. Модели и методы организационного управления информационными рисками корпораций. М.: Эгвес, 2011. 312 с.
8. Калашников А. О. Организационные механизмы управления информационными рисками корпораций. М.: ПМСОФТ, 2008. 175 с.
9. Xin Y., Kong L., Liu Z., Chen Y., Li Y., Zhu H., Wang C. Machine learning and deep learning methods for cybersecurity. *IEEE Access*. 2018. Vol. 6. Pp. 35365–35381.
10. Apruzzese G., Colajanni M., Ferretti L., Guido A., Marchetti M. On the effectiveness of machine and deep learning for cyber security. 2018 10th International Conference on Cyber Conflict. *IEEE*. 2018. Pp. 371–390.
11. Wickramasinghe C. S., Marino D. L., Amarasinghe K., Manic M. Generalization of deep learning for cyber-physical system security: A survey IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society. *IEEE*. 2018. Pp. 745–751.
12. Лиса Н. К., Сікора Л. С., Ткачук Р. Л., Тупичак Л. Л., Таланчук Р. Р., Федина Б. І., Федевич О. Ю. Інформаційні та когнітивні технології оцінки ситуації в автоматизованих системах управління в умовах дії завад і факторів збою. *Комп'ютерні технології друкарства*. 2021. № 1 (45). С. 110–130.
13. Джус В. Проектування реплікатора для координування пакетів даних у малому поліграфічному підприємстві. Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку : матеріали Всеукраїнської науково-практичної Інтернет-конференції. Черкаси, 2016. С. 40–41.
14. Дурняк Б. В., Сікора Л. С., Лиса Н. К., Якимчук Б. Л. Інформаційні технології для узгодження і координації людино – машинних систем оперативного управління ієрархічними структурами. *Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова*. 2014. № 71. С. 42–54.
15. Дурняк Б. В. Пристрої та системи цифрового друку. Львів : Фенікс, 2002. 106 с.
16. Баранкевич М. М. Експертні методи в ухвалені рішень. Львів : ВЦ ЛНУ ім. І. Франка, 2008. 214 с.

17. Шепіта П. І. Аналіз обчислювальних платформ для організації збору даних на виробництві. Тези доповідей студентської науково-технічної конференції УАД. Львів, 2017. С. 11.
18. Шепіта П. І. Класифікація систем контролю та управління робочими процесами на підприємстві. Тези доповідей студентської науково-технічної конференції. Львів, 2016. С. 24.
19. Шепіта П. І. Моніторинг якості кольоропередачі при потоковому опрацюванні даних штучною нейронною мережею. Сучасні методи, інформаційне, програмне та технічне забезпечення систем керування організаційно-технічними та технологічними комплексами. Матеріали V Міжнародної науково-технічної конференції. Київ, 2018. С. 226–227.
20. Кремса О. Р. Забезпечення віддаленої синхронізації кінцевих користувачів в процесі виконання замовлення. Матеріали доповідей студентської наукової конференції. Львів, 2017. С. 8.
21. Лях І. М., Білак Ю. Ю., Даньков-Товтин Л. Я., Станишевський В. В. Використання перевірки статистичних гіпотез в інформаційно-технічній сфері A/B тестування та доцільність його застосування. *Квалілогія книги.* 2015. № 2 (28). С. 82–85.
22. Шепіта П. І. Оцінювання якості проектування інтерфейсу користувача віртуальної лабораторії для технічних спеціальностей. *Комп'ютерні технології друкарства.* 2021. № 1 (45). С. 73–80.
23. Шепіта П. І. Побудова блок–схеми регулювання температурних показників з використанням штучних нейронних мереж. Фізика, Електроніка, Електротехніка: ФЕЕ-2020: матеріали міжнародної науково-технічної конференції студентів та молодих вчених. Суми, 2020. С. 196.
24. Шепіта П. І. Побудова структури інтелектуального управління технологічними процесами поліграфічного цеху. Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: матеріали всеукраїнської науково-технічної конференції. Черкаси, 2020. С. 7–9.
25. Кремса О. Р. Обмеження прав доступу різнорівневих користувачів під час створення веб-сервісу малого друкарського підприємства. Автоматизація та комп'ютерно інтегровані технології у виробництві та освіті:стан, досягнення, перспективи розвитку: праці Всеукраїнської науково-практичної конференції. Черкаси, 2017. С. 94–96.
26. Шепіта П. І. Розширення корпоративної бази даних для інтегрування виробничої телеметрії в навчальний експеримент. Матеріали XVIII міжнародної науково-технічної конференції студентів та аспірантів «Друкарство молоде». Київ, 2018. С. 59–61.
27. Шепіта П. І. Інформаційна модель системи інтелектуального координування процесів друкарського цеху. *Моделювання та інформаційні технології.* 2019. № 86. С. 91–95.
28. Shepita P. Evaluation of the quality of polygraphic equipment work at the streaming data processing by the artificial neural network. «Information technologies of printing» DRUKOTECHN-2018: a collection of scientific proceedings of the VII International Scientific and Technical Conference. Lviv, 2018. Pp. 110–111.
29. Шепіта П. І. Проектування нейрорегулятора температурного режиму для поліграфічного обладнання. Сучасні методи, інформаційне, програмне та технічне забезпечення

систем керування організаційно-технічними та технологічними комплексами. Матеріали V Міжнародної науково-технічної конференції. Київ, 2019. С. 182.
30. Goodall N. Non-technological challenges for the remote operation of automated vehicles. *Transportation Research*. 2020. Vol. 142. Pp. 14–26.
31. ISO/TS 15311-2:2018. Graphic technology — Print quality requirements for printed matter — Part 2: Commercial print applications utilizing digital printing technologies.
32. Шепіта П. І. Інформаційна модель динамічного вебсервісу інтелектуальної системи управління. *Комп'ютерні технології друкарства*. 2019. № 2 (42). С. 73–80.
33. Шепіта П. І. Розробка алгоритмічних засобів координування виробничого процесу. Матеріали XVII наукової конференції «Друкарство молоде». Київ, 2017. С. 49–51.
34. Шепіта П. І. Технологія прийняття управлінських рішень в системі інтелектуального управління виробничими процесами. Поліграфічні, мультимедійні та web-технології (PMW-2020): матеріали V міжнародної науково-технічної конференції. Київ, 2020. С. 57–59.
35. Баранкевич М. М. Експертні методи в ухвалені рішень. Львів : ВЦ ЛНУ ім. І. Франка. 2008. 214 с.
36. Сікора Л. С., Дурняк Б. В., Антоник М. С., Ткачук Р. Л. Когнітивні моделі формування стратегій оперативного управління інтегрованими ієрархічними структурами в умовах ризиків і конфліктів. Львів : Українська академія друкарства, 2013. 449 с.
37. Sikora L., Tkachuk R., Lysa N. Dronyuk I., Fedevych O., Navutka M. Information technologies of formation of intellectual decision-making strategies under conditions of cognitive failures. 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems (CITRisk – 2020). Cherson, Ukraine, Octovber 15–16, 2020. Vol. 2805. Pp. 233–254.
38. Sikora L., Tkachuk R., Lysa N., Dronyuk I., Fedevych O. Information and Logic Cognitive Technologies of Decision-making in Risk Conditions. IntellTSIS 2020. Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. (CEUR-WS.org, ISSN 1613-0073) Khmelnytskyi, Ukraine, June 10–12, 2020. Vol. 2623. Pp. 340–356.
39. Сікора Л. С., Лиса Н. К., Ткачук Р. Л., Навитка М. Л., Сабат В. І., Федина Б. І., Тупичак Л. Л. Інформаційні технології формування стратегій прийняття рішень інтелектуальним агентом в техногенних системах за умов когнітивних збоїв. *Комп'ютерні технології друкарства*. 2020. No 1 (43). С. 71–94.
40. Ажмухамедов И. М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования. Астрахань, 2012. 344 с.
41. Федулов А. С. Нечеткие реляционные когнитивные карты. *Теория и системы управления.* 2005. № 1. С. 120–132.
42. Баскаков А. В., Остапенко А. Г., Щербаков В. Б. Политика информационной безопасности как основной документ организации. *Информация и безопасность.* 2016. № 2. С. 43–47.
43. Борисова К. В., Кудашкин Я. В. Международная информационная безопасность как основополагающий фактор национальной безопасности. *Национальная безопасность:*

противодействие экстремизму и терроризму и перспективы преодоления глобальных проблем. 2016. С. 68–73.

44. Сікора Л. С., Лиса Н. К., Тупичак Л. Л., Сабат В. І., Навитка Л. М. Інформаційно-когнітивні концепції процесів інтелектуальної діяльності особи під час прийняття рішень у кризових умовах. *Наукові записки [Української академії друкарства]*. 2019. No 2 (59). С. 80–89.

REFERENCES

1. Durniak, B. V., Sabat, V. I., & Shvedova, L. Ye. (2016). Upravlinnia povnovazhenniamy v systemakh zakhystu informatsii. Lviv : UAD (in Ukrainian).
2. Sabat, V. I., Matsiuk, V. V., Musiiovska, M. M., & Kanevska, N. I. (2020). Rozroblennia systemy upravlinnia dostupom do dokumentiv v ASDO dlia polihrafichnykh vydavnytstv: Naukovi zapysky [Ukrainskoi akademii drukarstva], 2 (60), 68–74 (in Ukrainian).
3. Shepita, P. I. (2019). Informatsiina model dynamichnoho vebservisu intelektualnoi systemy upravlinnia: Komp'iuterni tekhnolohii drukarstva, 2 (42), 73–80 (in Ukrainian).
4. Shepita, P. I. (2018). Syntez informatsiinoi modeli intelektualnoho upravlinnia polihrafichnym vyrobnytstvom na osnovi shtuchnykh neironnykh merezh: Modeliuvannia ta informatsiini tekhnolohii, 85, 192–196 (in Ukrainian).
5. Sabat, V. I., & Shepita, P. I. (2018). Funktsionalna model systemy zakhystu avtomatyzovanoi systemy dokumentoobihu: Modeliuvannia ta informatsiini tekhnolohii, 84, 190–195 (in Ukrainian).
6. Kalashnikov, A. O. (2004). Upravlenie informacionnymi riskami s ispol'zovaniem arbitrazhnyh shem: Sistemy upravlenija i informacionnye tehnologii, 4 (16), 57–61 (in Russian).
7. Kalashnikov, A. O. (2011). Modeli i metody organizacionnogo upravlenija informacionnymi riskami korporacij. M.: Jegves (in Russian).
8. Kalashnikov, A. O. (2008). Organizacionnye mehanizmy upravlenija informacionnymi riskami korporacij. M.: PMSOFT (in Russian).
9. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity: IEEE Access, 6, 35365–35381 (in English).
10. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. 2018 10th International Conference on Cyber Conflict: IEEE, 371–390 (in English).
11. Wickramasinghe, C. S., Marino, D. L., Amarasinghe K., & Manic, M. (2018). Generalization of deep learning for cyber-physical system security: A survey IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society: IEEE, 745–751 (in English).
12. Lysa, N. K., Sikora, L. S., Tkachuk, R. L., Tupychak, L. L., Talanchuk, R. R., Fedyna, B. I., & Fedevych, O. Yu. (2021). Informatsiini ta kohnityvni tekhnolohii otsinky sytuatsii v avtomatyzovanykh systemakh upravlinnia v umovakh dii zavad i faktoriv zboiu: Komp'iuterni tekhnolohii drukarstva, 1 (45), 110–130 (in Ukrainian).
13. Dzhus, V. (2016). Proektuvannia replikatora dlia koordynuvannia paketiv danykh u malomu polihrafichnomu pidpryiemstvi. Avtomatyzatsiia ta komp'iuterno-intehrovani tekhnolohii u vyrobnytstvi ta osviti: stan, dosiahnennia, perspektyvy rozvytku : materialy Vseukrainskoi naukovo-praktychnoi Internet-konferentsii. Cherkasy, 40–41 (in Ukrainian).

14. Durniak, B. V., Sikora, L. S., Lysa, N. K., & Yakymchuk, B. L. (2014). Informatsiini tekhnolohii dlia uzghodzhennia i koordynatsii liudyno – mashynnykh system operatyvnoho upravlinnia iierarkhichnymy strukturamy: Zbirnyk naukovykh prats Instytutu problem modeliuvannia v enerhetytsi im. H. Ye. Pukhova, 71, 42–54 (in Ukrainian).
15. Durniak, B. V. (2002). Prystroi ta systemy tsyfrovoho druku. Lviv : Feniks (in Ukrainian).
16. Barankevych, M. M. (2008). Ekspertni metody v ukhvaleni rishen. Lviv : VTs LNU im. I. Franka (in Ukrainian).
17. Shepita, P. I. (2017). Analiz obchysliuvalnykh platform dlia orhanizatsii zboru danykh na vyrobnytstvi. Tezy dopovidei studentskoi naukovo-tekhnichnoi konferentsii UAD. Lviv (in Ukrainian).
18. Shepita, P. I. (2016). Klasyfikatsiia system kontroliu ta upravlinnia robochymy protsesamy na pidpryiemstvi. Tezy dopovidei studentskoi naukovo-tekhnichnoi konferentsii. Lviv (in Ukrainian).
19. Shepita, P. I. (2018). Monitorynh yakosti koloroperedachi pry potokovomu opratsiuvanni danykh shtuchnoiu neironnoiu merezheiu. Suchasni metody, informatsiine, prohramne ta tekhnichne zabezpechennia system keruvannia orhanizatsiino-tekhnichnymy ta tekhnolohichnymy kompleksamy. Materialy V Mizhnarodnoi naukovo-tekhnichnoi konferentsii. Kyiv, 226–227 (in Ukrainian).
20. Kremsa, O. R. (2017). Zabezpechennia viddalenoi synkhronizatsii kintsevykh korystuvachiv v protsesi vykonannia zamovlennia. Materialy dopovidei studentskoi naukovoi konferentsii. Lviv, 8 (in Ukrainian).
21. Liakh, I. M., Bilak, Yu. Yu., Dankov-Tovtyn, L. Ya., & Stanyshevskyi, V. V. (2015). Vykorystannia perevirky statystychnykh hipotez v informatsiino-tekhnichnii sferi A/V testuvannia ta dotsilnist yoho zastosuvannia: Kvalilohiia knyhy, 2 (28), 82–85 (in Ukrainian).
22. Shepita, P. I. (2021). Otsiniuvannia yakosti proektuvannia interfeisu korystuvacha virtualnoi laboratorii dlia tekhnichnykh spetsialnostei: Komp'iuterni tekhnolohii drukarstva, 1 (45), 73–80 (in Ukrainian).
23. Shepita, P. I. (2020). Pobudova blok–skhemy rehuliuvannia temperaturnykh pokaznykiv z vykorystanniam shtuchnykh neironnykh merezh. Fizyka, Elektronika, Elektrotekhnika: FEE-2020: materialy mizhnarodnoi naukovo-tekhnichnoi konferentsii studentiv ta molodykh vchenykh. Sumy (in Ukrainian).
24. Shepita, P. I. (2020). Pobudova struktury intelektualnoho upravlinnia tekhnolohichnymy protsesamy polihrafichnoho tsekhu. Avtomatyzatsiia ta komp'iuterno-intehrovani tekhnolohii u vyrobnytstvi ta osviti: materialy vseukrainskoi naukovo-tekhnichnoi konferentsii. Cherkasy, 7–9 (in Ukrainian).
25. Kremsa, O. R. (2017). Obmezhennia prav dostupu riznorivnevykh korystuvachiv pid chas stvorennia veb-servisu maloho drukarskoho pidpryiemstva. Avtomatyzatsiia ta komp'iuterno intehrovani tekhnolohii u vyrobnytstvi ta osviti:stan, dosiahnennia, perspektyvy rozvytku: pratsi Vseukrainskoi naukovo-praktychnoi konferentsii. Cherkasy, 94–96 (in Ukrainian).
26. Shepita, P. I. (2018). Rozshyrennia korporatyvnoi bazy danykh dlia intehruvannia vyrobnychoi telemetrii v navchalnyi eksperyment. Materialy XVIII mizhnarodnoi naukovo-tekhnichnoi konferentsii studentiv ta aspirantiv «Drukarstvo molode». Kyiv, 59–61 (in Ukrainian).

27. Shepita, P. I. (2019). Informatsiina model systemy intelektualnoho koordynuvannia protsesiv drukarskoho tsekhu: Modeliuvannia ta informatsiini tekhnolohii, 86, 91–95 (in Ukrainian).
28. Shepita, P. (2018). Evaluation of the quality of polygraphic equipment work at the streaming data processing by the artificial neural network. "Information technologies of printing" DRUKOTECHN-2018: a collection of scientific proceedings of the VII International Scientific and Technical Conference. Lviv, 110–111 (in English).
29. Shepita, P. I. (2019). Proektuvannia neirorehuliatora temperaturnoho rezhymu dlia polihrafichnoho obladnannia. Suchasni metody, informatsiine, prohramne ta tekhnichne zabezpechennia system keruvannia orhanizatsiino-tekhnichnymy ta tekhnolohichnymy kompleksamy. Materialy V Mizhnarodnoi naukovo-tekhnichnoi konferentsii. Kyiv, 182 (in Ukrainian).
30. Goodall, N. (2020). Non-technological challenges for the remote operation of automated vehicles: Transportation Research, 142, 14–26 (in English).
31. ISO/TS 15311-2:2018. Graphic technology — Print quality requirements for printed matter — Part 2: Commercial print applications utilizing digital printing technologies (in English).
32. Shepita, P. I. (2019). Informatsiina model dynamichnoho vebservisu intelektualnoi systemy upravlinnia: Komp'iuterni tekhnolohii drukarstva, 2 (42), 73–80 (in Ukrainian).
33. Shepita, P. I. (2017). Rozrobka alhorytmichnykh zasobiv koordynuvannia vyrobnychoho protsesu. Materialy XVII naukovoi konferentsii «Drukarstvo molode». Kyiv, 49–51 (in Ukrainian).
34. Shepita, P. I. (2020). Tekhnolohiia pryiniattia upravlinskykh rishen v systemi intelektualnoho upravlinnia vyrobnychymy protsesamy. Polihrafichni, multymediini ta web-tekhnolohii (PMW-2020): materialy V mizhnarodnoi naukovo-tekhnichnoi konferentsii. Kyiv, 57–59 (in Ukrainian).
35. Barankevych, M. M. (2008). Ekspertni metody v ukhvaleni rishen. Lviv : VTs LNU im. I. Franka (in Ukrainian).
36. Sikora, L. S., Durniak, B. V., Antonyk, M. S., & Tkachuk, R. L. (2013). Kohnityvni modeli formuvannia stratehii operatyvnoho upravlinnia intehrovanymy iierarkhichnymy strukturamy v umovakh ryzykiv i konfliktiv. Lviv : Ukrainska akademiia drukarstva (in Ukrainian).
37. Sikora, L., Tkachuk, R., Lysa, N. Dronyuk, I., Fedevych, O., & Navutka, M. (2020). Information technologies of formation of intellectual decision-making strategies under conditions of cognitive failures. 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems (CITRisk – 2020). Cherson, Ukraine, Octovber 15–16, 2805, 233–254 (in English).
38. Sikora, L., Tkachuk, R., Lysa, N., Dronyuk, I., & Fedevych, O. (2020). Information and Logic Cognitive Technologies of Decision-making in Risk Conditions. IntellTSIS 2020. Proceedings of the 1st International Workshop on Intelligent Information Technologies & Systems of Information Security. (CEUR-WS.org, ISSN 1613-0073) Khmelnytskyi, Ukraine, June 10–12, 2623, 340–356 (in English).
39. Sikora, L. S., Lysa, N. K., Tkachuk, R. L., Navytka, M. L., Sabat, V. I., Fedyna, B. I., & Tupychak, L. L. (2020). Informatsiini tekhnolohii formuvannia stratehii pryiniattia rishen intelektualnym ahentom v tekhnohennykh systemakh za umov kohnityvnykh zboiv: Komp'iuterni tekhnolohii drukarstva, 1 (43), 71–94 (in Ukrainian).

40. Azhmuhamedov, I. M. (2012). Reshenie zadach obespechenija informacionnoj bezopasnosti na osnove sistemnogo analiza i nechetkogo kognitivnogo modelirovanija. Astrahan' (in Russian).
41. Fedulov, A. S. (2005). Nechetkie reljacionnye kognitivnye karty: Teorija i sistemy upravlenija, 1, 120–132 (in Russian).
42. Baskakov, A. V., Ostapenko, A. G., & Shherbakov, V. B. (2016). Politika informacionnoj bezopasnosti kak osnovnoj dokument organizacii: Informacija i bezopasnost', 2, 43–47 (in Russian).
43. Borisova, K. V., & Kudashkin, Ja. V. (2016). Mezhdunarodnaja informacionnaja bezopasnost' kak osnovopolagajushhij faktor nacional'noj bezopasnosti: Nacional'naja bezopasnost': protivodejstvie jekstremizmu i terrorizmu i perspektivy preodolenija global'nyh problem, 68–73 (in Russian).
44. Sikora, L. S., Lysa, N. K., Tupychak, L. L., Sabat, V. I., & Navytka, L. M. (2019). Informatsiino-kohnityvni kontseptsii protsesiv intelektualnoi diialnosti osoby pid chas pryiniattia rishen u kryzovykh umovakh: Naukovi zapysky [Ukrainskoi akademii drukarstva], 2 (59), 80–89 (in Ukrainian).

doi: 10.32403/0554-4866-2021-2-82-74-91

USING LOGICAL-COGNITIVE APPROACHES TO INFORMATION PROTECTION IN AUTOMATIC ORDERING AT PRINTING COMPANIES

P. I. Shepita, L. L. Tupychak

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
reboot1804@ukr.net

The subject of scientific works on introduction of modern technologies and systems of automated management of the company, its resources and technical means is analysed and insufficient completeness of researches on features of the complex approach at designing and deployment of innovative means of the production order support is shown. On the basis of certain factors of the company functioning in the newest conditions of the fourth industrial revolution the directions of strategies formation of elements introduction of Industry 4.0 in modern printing companies, and also systems of the information protection at electronic document circulation are caused.

Mechanisms for solving the problems of information risk management in complex management systems of printing enterprises in conditions of uncertainty and in the event of mutual influence of the management system elements on each other are considered. The necessity of using the web portal for formation of printing orders is substantiated, the main components are defined and the levels of access to them are described.

To increase the efficiency of information security of the company intelligent management system, one of the logical-cognitive directions is used - fuzzy logical-cognitive model, which consists in combining the information about the content of threats, vulnerabilities and means of protection. The proposed approaches allowed one to consider the impact of potential attacks on basic information security services. In the process, the principles of information protection in human-independent systems in the automated processing of orders at printing companies are substantiated, based on logical-cognitive methods of assessing the quality of minimizing the risk of loss or modification of information and illegal data acquisition.

Keywords: *intelligent control system, web portal, order, non-clear logical-cognitive model, information protection.*

Стаття надійшла до редакції 28.09.2021.
Received 28.09.2021.