ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ТЕОРІЯ КОДУВАННЯ

УДК 004.4'277.2.056.55

А. О. Азарова, І. О. Дьогтєва, А. А. Шиян

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Вінницький національний технічний університет, Вінниця

Анотація. У статті запропоновано систему підтримки прийняття рішень (СППР) щодо підвищення рівня інформаційної безпеки вітчизняних підприємств, яка уможливлює індивідуальний підбір методів та засобів такої політики на основі експертних даних, а також з урахуванням побажань суб'єкта господарювання. Було визначено та обґрунтовано її структуру; здійснено програмну реалізацію такої СППР для адаптивного підбору методів та засобів політики інформаційної безпеки. Основними функціями СППР щодо підвищення рівня інформаційної безпеки підприємства є: автентифікація користувачів, оцінювання незалежним експертом з інформаційної безпеки пріоритетності захисту від можливих або потенційних загроз; можливість користувачу самостійно обирати найбільш поширені для підприємства загрози щодо яких необхідно вжити специфічний захист; пропозиція користувачеві найбільш відповідних методів політики інформаційної безпеки з урахуванням усіх його побажань; динамічне оновлення даних із метою забезпечення спостереження за новітніми методами захисту. Наукова новизна отриманих результатів полягає в тому, що вперше розроблено систему підтримки прийняття рішень, що дозволяє засобами системного підходу та ER-моделювання суттєво підвищити рівень інформаційної безпеки підприємства, здійснюючи індивідуальний підбір методів та засобів політики інформаційної безпеки на підприємстві на основі побажань підприємця та експертних оцінок.

Ключові слова: інформаційна безпека підприємств, загрози інформаційній безпеці, політика інформаційної безпеки, система підтримки прийняття рішень, ER-моделювання.

Abstract. The article proposes a decision support system (DSS) to increase the level of information security of domestic enterprises, which allows individual selection of methods and tools of such a policy based on expert data, as well as taking into account the wishes of the business entity. Its structure was determined and substantiated; program implementation of such DSS for adaptive selection of methods and means of information security policy was carried out. The main functions of such DSS to increase the level of information security of the enterprise are: user authentication; assessment by an independent information security expert of the priority of protection against possible or potential threats; the ability of the user to choose the most common threats to the company for which it is necessary to take specific protection; offer the user the most appropriate methods of information security policy, taking into account all his wishes; dynamic data update to monitor the latest security methods. The scientific novelty of the obtained results is that it was developed for the first the DSS which allows to increase the level of information security of the enterprise by means of system technique and ER-modelling and to select individual methods and tools of information security policy of enterprise based on the wishes of the entrepreneur and expert assessments text.

Key words: information security of enterprises, threats to information security, information security policy, decision support system, ER-modelling.

DOI: https://doi.org/10.31649/1999-9941-2022-53-1-12-18.

Вступ

Процеси глобалізації інформаційної сфери та цифрової трансформації, розвиток інформаційного суспільства, впровадження передових інформаційно-комунікаційних технологій, нових видів продукції та послуг формують новітні суспільні відносини у різних сферах життєдіяльності людини в межах суспільства, держави та світу. Вони породжують нові виклики і загрози у сфері інформаційної та кібернетичної безпеки на національному та міжнародному рівнях. Наразі, з розвитком інформаційного суспільства на порядку денному розвиток цифрової економіки [1], що передбачає наявність ринкових стимулів, мотивацій, попиту та необхідності використання цифрових технологій, продуктів і послуг секторами промисловості, бізнесу та суспільства для забезпечення, насамперед, їх конкурентоздатності та ефективності, реалізації зростання обсягів виробництва з метою збільшення прибутковості [2].

Нарощування масштабу і темпу цифрових трансформацій відбувається паралельно зі зростанням кількості та номенклатури кібератак. Особливо порушення інформаційної безпеки спостерігається на мікрорівні, а саме на рівні підприємств. Основні інтереси організацій на сьогодні значною мірою визначаються саме станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки загалом. Саме тому інформаційна безпека є необхідною та невід'ємною умовою для правильного і безперервного функціонування підприємства.

Актуальність

Загалом проблематикою захисту інформації займаються провідні закордонні та вітчизняні науковці, серед яких слід відзначити Дж. Уілсона, Додонова О. Г., Карпінця В. В., Ланде Д. В., Лужецького В. А., Новікова О. М., Торокіна О. О., Хорєва О. О., Хорошка В. О., Шелеста М. Є., Яремчука Ю. Є. та ін.

Проблеми формування політики інформаційної безпеки (ПІБ) на підприємствах висвітлюються у роботах багатьох зарубіжних та українських вчених, таких як В. М. Богуш, О. К. Юдін, О. Л. Голубенко, Ленков С. В., Перегудов Д. А., Петров А. А., Соколов А. В. та ін [3-6]. У них обґрунтовано критерії оці-

нювання ризиків інформаційній безпеці підприємств залежно від категорій інформації, яка циркулює в них, пропонуються структури та ієрархії ПІБ, розглядаються внутрішні та зовнішні загрози, описуються випадки зловмисних дій і пропонуються можливі варіанти запобігань та санкцій проти них.

Не зважаючи на значний науковий доробок у цій царині знань, досить мало уваги приділяється саме індивідуальному підбору засобів та методів ПІБ суб'єктів господарювання різних галузей, форм власності та величини.

Необхідність адаптувати ПІБ під конкретне підприємство зумовлюється низкою чинників, серед яких потреба у доволі високій оплаті послуг безпеки, які надаються сторонніми виконавцями або внутрішніми спеціалістами; низький рівень компетентності пересічних працівників у сфері безпеки загалом та розумінні існуючих методів і підходів до формування ПІБ, зокрема; вразливості відомих методів, які лише в загальному відповідають задачам інформаційного захисту конкретних підприємств.

Застосування систем підтримки прийняття рішень уможливлює ґрунтовний та об'єктивний аналіз сфери інформаційної безпеки для формування оптимальної політики захисту інформації на підприємстві. Таким чином, актуальним є розроблення відповідної адаптованої до вимог суб'єкта господарювання ПІБ з використанням сучасних програмних засобів, зокрема, СППР.

Мета

Метою статті є удосконалення ПІБ на підприємстві шляхом розроблення відповідної СППР, яка дозволяє здійснити індивідуально орієнтований підбір методів та засобів захисту на основі експертних даних, а також з урахуванням побажань суб'єкта господарювання (підприємця).

Задачі

1. Визначити структуру СППР щодо підвищення рівня інформаційної безпеки на підприємстві.
2. Програмно реалізувати СППР для адаптивного підбору методів та засобів ПІБ на базі експертних даних, які враховують потреби підприємства шляхом вибору.

Структурне та організаційне моделювання СППР щодо підвищення рівня інформаційної безпеки на підприємстві

У загальному вигляді вимоги до СППР для виявлення ознак загроз інформаційній безпеці підприємств та оцінювання їх рівня сформульовано, насамперед, у міжнародних стандартах ISO серій 9000, 14000, 27000 [7-9].

Стандарт ISO 27001 [10] формулює вимоги у галузі інформаційної безпеки щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою. У стандарті наголошується на стратегічності рішення організації щодо прийняття системи управління інформаційною безпекою та перераховуються фактори впливу на створення та впровадження такої системи: потреби та цілі організації; вимоги до безпеки; процеси, які протікають у межах організації; архітектура (розмір, структура) організації.

Стандарти [7-10] демонструють узгодженість між собою і ґрунтуються на процесному підході до побудови систем управління. Суть процесного підходу зводиться до опису функціонування системи як набору взаємозалежних неперервних дій.

В основу даних міжнародних стандартів покладено модель PDCA (цикл Шухарта-Демінга) – структуру життєвого циклу усіх процесів системи [11]. Сутність моделі зводиться до неперервного покращення процесів, що забезпечує ефективне керування функціонуванням на системній основі.

Тому до СППР для виявлення ознак загроз інформаційній безпеці підприємства та оцінювання їх рівня висуваються вимоги щодо відповідності серії міжнародних стандартів ISO, моделі PDCA [11] і процесному підходу [7-10].

Процес розроблення та реалізації СППР щодо підвищення рівня інформаційної безпеки на підприємстві складається з таких послідовних етапів [12]: постановка задачі, формулювання вимог до створення проекту СППР, опис програмної реалізації та програмування модулів системи, тестування системи, підготовка інсталяційної версії і експлуатаційної документації, впровадження системи на технічних засобах замовника, супровід СППР (полягає, насамперед, у заключному виправленні помилок на етапі експлуатації системи, адаптаційному розширенні та модифікації функцій).

До складу СППР щодо підвищення рівня інформаційної безпеки на підприємстві входять три головні компоненти: база даних (БД), база моделей та програмна підсистема, яка складається з трьох підсистем: системи управління базою даних, системи управління базою моделей і системи управління інтерфейсом між користувачем і комп'ютером.

До складу БД, які використовуються для аналізу і звернення до даних, належить мова опису даних (МОД) і мова маніпулювання даними (ММД) [13]. МОД дає можливість визначити структуру БД, де опис даних заданої проблемної області може виконуватися на кількох рівнях абстрагування, для яких характерна власна ММД, яка забезпечує доступ до даних та по суті реалізує запити.

СППР, що пропонується, має трирівневу систему: концептуальний (формується концептуальна схема із зазначенням взаємозв'язків між системами даних, які відповідають реально діючим залежностям

між факторами і параметрами проблемного середовища), логічний (взаємозв'язки, представлені у структурі записів БД) і фізичний рівень (розміщення структури записів на фізичних носіях інформації).

Концептуальну схему СППР щодо підвищення рівня інформаційної безпеки на підприємстві представлено у вигляді ER-моделі, яка дозволяє описувати дані за допомогою узагальнених конструкцій блоків. У випадку СППР, що пропонується (рис. 1), маємо сутності користувача (керівник або відповідальна особа на підприємстві) та комплексу даних (БД для реалізації забезпечення інформаційної безпеки на підприємстві).

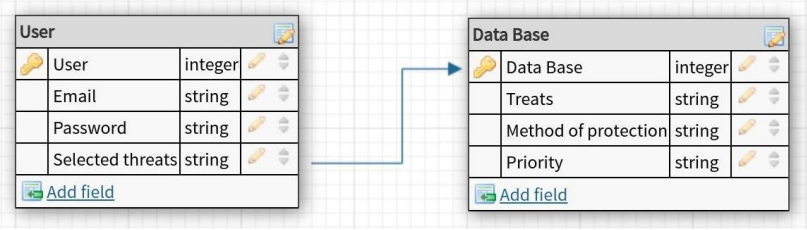

Рисунок 1 – ER-модель СППР щодо підвищення рівня інформаційної безпеки на підприємстві

Сутності мають різні властивості (атрибути), які формують притаманні їм характеризуючий та функціональний пакети. Користувачу, крім персональної інформації, що використовується під час авторизації та автентифікації, надана можливість вибору з переліку загроз актуальних на даний момент часу. Комплекс даних відповідає методам захисту, обраним користувачем загрозам і містить сортуючий пріоритетний список (рис. 1).

Логічний рівень представлено блок-схемою алгоритму програмного продукту (рис. 2).

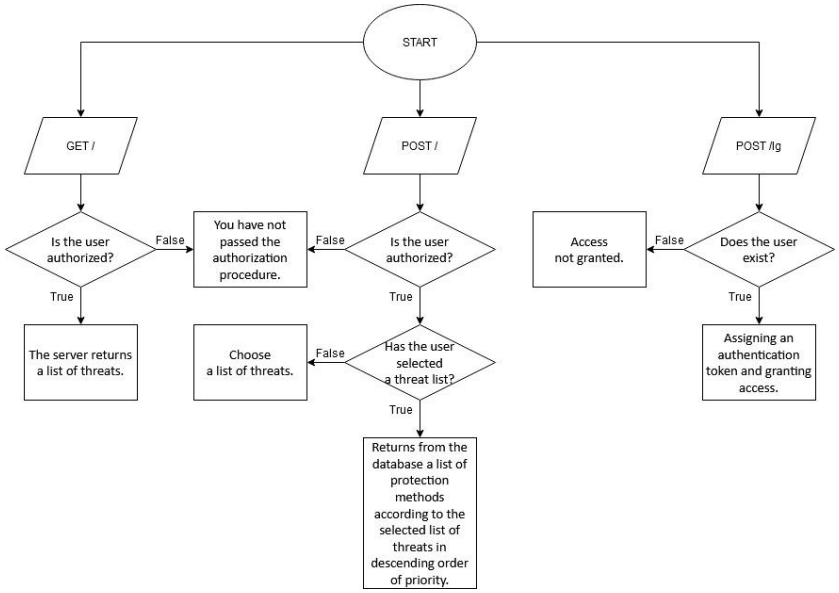

Рисунок 2 – Блок-схема алгоритму програмного продукту для СППР

СППР отримують інформацію з управлінських і операційних інформаційних систем. Дані, які акумульовані в БД, можуть використовуватися безпосередньо користувачем для розрахунків за допомогою математичних моделей.

Зв'язок кінцевих користувачів із БД відбувається за допомогою СУБД. Вона представлена як система програмного забезпечення, що містить засоби оброблення мовами БД. СУБД реалізує створення БД, відповідає за її цілісність, підтримку в активному стані, дає можливість маніпулювати даними, обробляти звернення до БД, які надходять від прикладних програм і кінцевих користувачів із застосованням технології оброблення інформації. Загалом СУБД, що розробляється, забезпечує: формування комбінацій даних із різних джерел за допомогою процедур агрегування і фільтрації; швидке додавання або вилучення джерела даних; побудову логічної структури даних у термінах користувача; використання і маніпуляцію неофіційними даними для експериментального оброблення альтернатив користувача; повну логічну незалежність даної БД від інших операційних БД [14], які функціонують на даному підприємстві.

Варто зауважити, що, порівняно зі звичайними підходами до реалізації БД, для вирішення деяких завдань щодо функцій та інструментів БД і СУБД у контексті розроблюваної СППР висувається ряд додаткових і спеціалізованих вимог.

Умовою використання СППР, що розробляється, є необхідність доступу інформації зі значно ширшого діапазону джерел, ніж це передбачено у звичайних інформаційних системах. Це пояснюється тим, що інформація отримується від зовнішнього середовища і внутрішніх джерел; крім того, звичайні, орієнтовані на бухгалтерський облік, дані. Тому, запропоновану СППР було доповнено нетрадиційними типами даних, зокрема, текстовою інформацією та ін.

Заслуговує також на увагу особливість процесу «Пошуку і захоплення» даних у СППР щодо підвищення рівня інформаційної безпеки на підприємстві. Процес пошуку, власне, як і сама СУБД, яка керує цим процесом, є досить гнучкими, щоб швидко обслуговувати доповнення і зміни відповідно до непередбачених запитів, які надходять від користувачів. Тому, для процесу «Пошуку і збільшення» даних у СППР, що розробляється, застосовуються програмні агенти.

Дані беруться з різноманітних джерел оперативних даних. Після їх переміщення відбираються лише суттєві дані, що є безперервними і точними. Потім дані завантажуються до реляційної таблиці, яка здатна підтримувати різноманітні види аналізу та запитів, і оптимізуються для тих таблиць, які найчастіше використовуватимуться. І, врешті-решт, дані зберігаються для подальшого використання у СППР.

Властивий СППР щодо підвищення рівня інформаційної безпеки на підприємстві акцент на оброблення неструктурованих і слабоструктурованих задач, до яких і належить формування індивідуальної політики захисту на підприємстві (з урахування уподобань замовника та низки експертних оцінок), зумовлює деякі специфічні вимоги до цих елементів комп'ютерної системи, що пропонується у статті.

Перш за все, мова йде про необхідність виконувати значний обсяг операцій переструктурування даних. Тому, пропонована СППР має можливість завантаження і наступного оброблення даних із зовнішніх джерел, що вимагає широкого набору функцій для функціонування СУБД.

У СППР щодо підвищення рівня інформаційної безпеки передбачено засіб, за допомогою якого користувач може налагоджувати базу даних відповідно до своїх особистих вимог. З огляду на це, використовуються процедури і команди гнучкого переструктурування схем і схемних підмножин СУБД. Зауважимо, що сучасні програмні засоби для управління даними і СУБД характеризуються відносною гнучкістю і простотою використання колективом користувачів. Проте, згадані засоби не можна пристосувати до конкретного користувача або до вирішення конкретного завдання з бажаною гнучкістю за умови малих витрат на такий процес.

Програмна реалізація СППР щодо підвищення рівня інформаційної безпеки на підприємстві

Для програмування авторського засобу було обрано оптимальну мову, якою (для вирішення такої задачі) є PHP, та фреймворк Laravel. Серед аргументів на користь такого вибору, слід зазначити: можливість засобами PHP генерувати HTML-сторінки на боці веб-сервера; інтерпретування її веб-сервером у HTML-код, який передається клієнту, причому користувач не бачить PHP-код, що є перевагою з точки зору безпеки; можливість підключення до всіх баз даних, до яких існує драйвер, завдяки стандарту відкритого інтерфейсу зв'язку з базами даних (Open Database Connectivity Standard, ODBC); вбудовані бібліотеки для роботи з MySQL, PostgreSQL, mSQL, Oracle, dbm, Hyperware, Informix, InterBase, Sybase; технічні переваги: висока продуктивність, функціональність посилань, використовується метод динамічних аргументів тощо. Серед пріоритетних особливостей обраного PHP-фреймворка з відкритим кодом, призначеного для розроблення веб-додатків відповідно до шаблону model-view-controller (MVC), слід виділити: модульну систему пакування з виділеним менеджером залежностей Composer, різні способи для доступу до реляційних баз даних, утиліти, які допомагають у розгортанні додатків і технічного обслуговування.

Функціонування даного продукту початково передбачає автентифікацію користувачів. Використано модель користувача, що надається за замовчуванням обраним фрейворком, яка дозволяє: під час створення користувача заповнити інформацію щодо імені, електронної адреси, паролю входу, приховати інформацію щодо паролю та токену в результатах запитів до БД.

Для вибору пріоритетів захисту об’єктам, що можуть потрапити під вплив загроз, авторами статті використано функцію PROTECTED. Функція виконується лише в разі авторизації користувача.

Під час роботи даного веб-застосунку користувач (керівник або відповідальна особа на підприємстві) обирає загрози інформаційній безпеці, які вже було зафіксовано в попередніх періодах функціонування підприємства, або ті, які вважаються пріоритетними для захисту.

На рис. 3 наведено фрагмент програмного коду, що описує звернення СППР щодо підвищення рівня інформаційної безпеки на підприємстві, до моделі загроз, яка функціонує в БД.

```php
namespace App;

use Illuminate\Database\Eloquent\Model;

class Threat extends Model {
    public function event() {
        return $this->hasMany('App\Event', 'threat_id', 'id');
    }
    public function events() {
        return $this->belongsToMany('App\Event');
    }
}
```

Рисунок 3 – Фрагмент коду звернення до моделі загроз у системі веб-застосунку СППР

Паралельно працює база даних з експертним оцінюванням пріоритетності всіх загроз. Після вибору найнебезпечніших загроз, користувачеві наводяться поради щодо впровадження та використання певних методів ПІБ, які задовольняють потреби конкретного підприємства.

Нижче представлено фрагмент програмного коду, в якому здійснюється доступ до контролера потенційних загроз, суттєвих для підприємства, що дозволяє розробити раціональну ПІБ (рис. 4).

```php
namespace App\Http\Controllers;
use App\Threat;
use Illuminate\Http\Request;
use Illuminate\Support\Facades\DB;

class ThreatController extends Controller {
    /**
    * @return \Illuminate\Http\Response
    */
    public function index() { }
    /**
    * @return \Illuminate\Http\Response
    */
    public function create() { }
    /**
    * @param \Illuminate\Http\Request $request
    * @return \Illuminate\Http\Response
    */
    public function store(Request $request) { }
    /**
    * @param \App\Threat $threat
    * @return \Illuminate\Http\Response
    */
    public function show(Threat $threat) { }
    /**
    * @param \App\Threat $threat
    * @return \Illuminate\Http\Response
    */
    public function edit(Threat $threat) { }
```

Рисунок 4 – Фрагмент коду доступу до контролера потенційних загроз у системі веб-застосунку СППР

У згенерованому контролері визначено низку методів для забезпечення динамічного функціонування. На рис. 5 продемонстровано процес оновлення після процедури запиту.

```php
    public function update(Request $request){
        $ids = $request->all();
        foreach ($ids as $key => $value) {
            $threat = Threat::find($key);
            $threat->priority = $value;
            $threat->save();
        }
        DB::table('event_threat')->delete();
        $threats = Threat::all();
        foreach ($threats as $threat) {
            $count_events = 9 - $threat->priority;
            $possible_events = $threat->event()->inRandomOrder()
                ->limit($count_events)->get()->pluck('id');
            $threat->events()->sync($possible_events);
        }
        return response()->json(['status' => 'OK'], 200);
    }
    /**
    * @param \App\Threat $threat
    * @return \Illuminate\Http\Response
    */
    public function destroy(Threat $threat) { }
}
```

Рисунок 5 – Фрагмент коду процесу оновлення після процедури запиту в системі веб-застосунку СППР

Розроблену СППР було протестовано. Це дозволило довести, що вона уможливлює спрощення процедури адекватного і об'єктивного вибору методів ПІБ керівником вітчизняного підприємства.

Висновки

Побудована СППР щодо підвищення рівня інформаційної безпеки підприємства має такі можливості: автентифікація користувачів; оцінювання незалежним експертом з інформаційної безпеки пріоритетності захисту від можливих або потенційних загроз; користувач може самостійно обирати поширені для підприємства загрози щодо яких необхідно вжити специфічний захист; надання переліку пропозицій користувачеві відповідних методів ПІБ з урахуванням усіх його побажань; динамічне оновлення даних із метою забезпечення спостереження за новітніми методами захисту.

Основний науковий результат полягає в тому, що вперше розроблено систему підтримки прийняття рішень, що дозволяє засобами системного підходу та ER-моделювання суттєво підвищити рівень інформаційної безпеки підприємства, здійснюючи індивідуальний підбір методів та засобів політики інформаційної безпеки на підприємстві на основі побажань підприємця та експертних оцінок.

Практичне значення результатів роботи полягає у розробленні програмного продукту, що дозволяє здійснювати індивідуальний підбір методів та засобів ПІБ на підприємстві на основі індивідуального вибору суб'єкта господарювання та застосування знань експертів.

Список літератури

[1] Кабінет Міністрів України. (2021, бер. 03). *Розпорядж. Каб. Міністрів України від 03.03.2021 р. № 167-р, Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації.* [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/167-2021-р#Text.

[2] Кабінет Міністрів України. (2018, січ. 17). *Розпорядж. Каб. Міністрів України від 17.01.2018 р. № 67-р : станом на 17 верес. 2020 р, Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації*. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/67-2018-р#Text.

[3] В. М. Богуш, О. К. Юдін, *Інформаційна безпека держави.* Київ, Україна: "МК-Прес", 2005.

[4] О. Л. Голубенко, В. О. Хорошко, О. С. Петров, С. М. Головань, Ю. Є. Яремчук, *Політика інформаційної безпеки. Практикум : навч. посібник.* Луганськ, Україна: СНУ ім. В. Даля, 2010.

[5] С. В. Ленков, Д. А. Перегудов, В. А. Хорошко, *Методы и средства защиты информации. В 2-х томах. Том I. Несанкционированное получение информации.* Київ, Україна: Арий, 2008.

[6] *С.* В. Ленков, Д. А. Перегудов, В. А. Хорошко, *Методы и средства защиты информации. В 2-х томах. Том II. Информационная безопасность* Київ, Україна: Арий, 2008.

[7] *ISO 9000:2015 Quality management systems − Fundamentals and vocabulary*. [Online]. Available: https://www.iso.org/ru/standard/45481.html. Accessed on: Jan. 4, 2021.

[8] *ISO/IEC 14001:2015 Environmental management systems – requirements with guidance for use*. [Online]. Available: https://www.iso.org/standard/60857.html. Accessed on: Jan. 4, 2021.

[9] *ISO/IEC 27000:2018 Information technology − Security techniques − Information security management systems − Overview and vocabulary*. [Online]. Available: https://www.iso.org/standard/73906.html. Accessed on: Jan. 4, 2021.

[10] *ISO/IEC 27001:2013 Information technology − Security techniques − Information security management systems − Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Jan. 4, 2021.

[11] Б. А. Кормич, *Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук : 12.00.07*. Харків, Україна, Національний університет внутрішніх справ, 2004.

[12] Г. М. Гнатієнко, В. Є. Снитюк, *Експертні технології прийняття рішень: Монографія.* Київ, Україна: ТОВ «Маклаут». – 2008.

[13] В. Р. Кігель, *Методи і моделі підтримки прийняття рішень у ринковій економіці: Монографія.* Київ, Україна: ЦУЛ, 2003.

[14] П. І. Бідюк, Л. О. Коршевнюк, *Проектування комп'ютерних інформаційних систем підтримки прийняття рішень: Навчальний посібник.* Київ, Україна: ННК „ІПСА" НТУУ „КПІ", 2010.

Стаття надійшла: 18.01.2022.

References

[1] *Rozporyadzh. Kab. Ministriv Ukrayiny vid 03.03.2021 r. № 167-r, Pro skhvalennya Kontseptsiyi rozvytku tsyfrovykh kompetentnostey ta zatverdzhennya planu zakhodiv z yiyi realizatsiyi* [Order of the Cabinet of Ministers of Ukraine dated 03.03.2021 № 167-r, On approval of the Concept of development of digital competencies and approval of the action plan for its implementation]. Available at: https://zakon.rada.gov.ua/laws/show/167-2021-r#Text [in Ukrainian].

[2] *Rozporyadzh. Kab. Ministriv Ukrayiny vid 17.01.2018 r. № 67-r : stanom na 17 veres. 2020 r, Pro skhvalennya Kontseptsiyi rozvytku tsyfrovoyi ekonomiky ta suspil'stva Ukrayiny na 2018-2020 roky ta zatverdzhennya planu zakhodiv shchodo yiyi realizatsiyi* [Order of the Cabinet of Ministers of Ukraine dated January 17, 2018 № 67-r: as of September 17. 2020, On approval of the Concept of Development of the Digital Economy and Society of Ukraine for 2018-2020 and approval of the action plan for its implementation]. Available at: https://zakon.rada.gov.ua/laws/show/67-2018-r#Text [in Ukrainian].

[3] Bohush, V. M., Yudin, O. K. *Informatsiyna bezpeka derzhavy* [Information security of the state]. Kyiv, "MK-Pres" Publ., 2005. 432 p. [in Ukrainian].

[4] Holubenko, O. L., Khoroshko, V. O., Petrov , O. S., Holovan', S. M., Yaremchuk, Yu. Ye. *Polityka informatsiynoyi bezpeky* [Information security policy]. Luhansk, SNU im. V. Dalya Publ., 2010. 208 p. [in Ukrainian].

[5] Lenkov S.V., Peregudov D.A., Khoroshko V.A. *Metody i sredstva zashchity informatsii. V 2-kh tomakh. Tom I. Nesanktsionirovannoe poluchenie informatsii* [Methods and means of information protection. In 2 volumes. Volume I. Unauthorized receipt of information]. Kyiv, Arii Publ., 2008. 464 p. [in Russian].

[6] Lenkov S.V., Peregudov D.A., Khoroshko V.A. *Metody i sredstva zashchity informatsii. V 2-kh tomakh. Tom II. Informatsionnaya bezopasnost'* [Methods and means of information protection. In 2 volumes. Volume II. Information Security]. Kyiv, Arii Publ., 2008. 344 p. [in Russian].

[7] *ISO 9000:2015 Quality management systems − Fundamentals and vocabulary.* Available at: https://www.iso.org/ru/standard/45481.html (accessed 04.01.2022).

[8] *ISO 14001:2015 Environmental management systems − Requirements with guidance for use.* Available at: https://www.iso.org/standard/60857.html (accessed 04.01.2022).

[9] *ISO/IEC 27000:2018 Information technology − Security techniques − Information security management systems − Overview and vocabulary.* Available at: https://www.iso.org/standard/73906.html (accessed 04.01.2022).

[10] *ISO/IEC 27001:2013 Information technology − Security techniques − Information security management systems − Requirements.* Available at: https://www.iso.org/standard/54534.html (accessed 01.12.2022).

[11] Kormych, B. A. *Orhanizatsiyno-pravovi osnovy polityky informatsiynoyi bezpeky Ukrayiny: Avtoref. dys. ... d-ra yuryd. nauk* [Organizational and legal bases of information security policy of Ukraine. Avtoref. diss. … doct. jurid. sci.]. Kharkiv, Natsional'nyy universytet vnutrishnikh sprav. Publ., 2004. 42 p. [in Ukrainian].

[12] Hnatiyenko, H.M., Snytyuk V.Ye. *Ekspertni tekhnolohiyi pryynyattya rishen'* [Expert decision-making technologies]. Kyiv, TOV «Maklaut» Publ., 2008. 444 p. [in Ukrainian].

[13] Kihel', V. R. *Metody i modeli pidtrymky pryynyattya rishen' u rynkoviy ekonomitsi* [Methods and models of decision support in a market economy]. Kyiv, TsUL Publ., 2003. 202 p. [in Ukrainian].

[14] Bidyuk, P. I., Korshevnyuk, L. O. *Proektuvannya komp"yuternykh informatsiynykh system pidtrymky pryynyattya rishen'* [Design of computer information systems for decision support]. Kyiv, NNK „IPSA" NTUU „KPI" Publ., 2010. 340 p. [in Ukrainian].

Відомості про авторів

Азарова Анжеліка Олексіївна – кандидат технічних наук, професор, професор кафедри менеджменту та безпеки інформаційних систем.

Дьогтєва Ірина Оксентіївна – асистент кафедри менеджменту та безпеки інформаційних систем.

Шиян Анатолій Антонович – кандидат фізико-математичних наук, доцент, доцент кафедри менеджменту та безпеки інформаційних систем.

A. O. Azarova, I. O. Dohtieva, A. A. Shyian

DECISION SUPPORT SYSTEM FOR INCREASING THE LEVEL OF INFORMATION SECURITY OF THE ENTERPRISE

Vinnytsia National Technical University, Vinnytsia