Огірко Ігор,
доктор фізико-математичних наук, професор,
доцент кафедри комп'ютерних наук та інформаційних технологій,
Житомирський державний університет імені Івана Франка,
м. Житомир, Україна
Огірко Ольга,
кандидат технічних наук, доцент,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів,
Львівський державний університет внутрішніх справ,
м. Львів, Україна
Кащевський Віктор,
здобувач третього (освітньо-наукового) рівня вищої освіти,
Львівський університет бізнесу та права
м. Львів, Україна

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В УПРАВЛІННІ ПІДПРИЄМСТВОМ

Розвиток інформаційних технологій на сучасному етапі дозволяє взаємодіяти підприємствам, спілкуватися співробітникам не тільки через дротові, а й через бездротові мережі та хмарні технології тому інформаційна безпека є головним чинником діяльності будь-якої організації, підприємства та кожної людини зокрема.

Інформаційні технології використовують на всіх етапах управління підприємством: планування ресурсів, постачання та збут, взаємодія з клієнтами, аналіз інформації, прийняття рішень. Найбільш поширеними інформаційними технологіями, які застосовуються в управлінні підприємством є: MRP (Material Requirements Planning), SCM (Supply Chain Management), HRM (Human Resources Management), CRM (Customer Relationship Management), ERP (Enterprise Resource Planning), BPR (Business Process Reengineering), MIS і BI (Management Information System and Business Intelligence).

На основі досліджень [2-5]. побудовано загальну структуру інформаційної технології управління підприємством.

Елементом загальної системи управління розглядають кібербезпеку підприємства, яка використовує методи, що враховують ризики інформаційної безпеки, як бізнес-ризики, та використовуються для створення, роботи, моніторингу, підтримування та вдосконалення заходів у сфері кібербезпеки.

За законом України «Про основні засади забезпечення кібербезпеки України», Кібербезпека – захищеність важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Кібербезпека в управлінні підприємства полягає в забезпеченні конфіденційності, *цілісності* та достовірності даних, які роблять діяльність організації безперебійною, та керується такими міжнародними стандартами та нормами: CoBiT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), ISO/IEC 27001:2005, ISO/IEC 17799, ISO/IES 15408 [5].

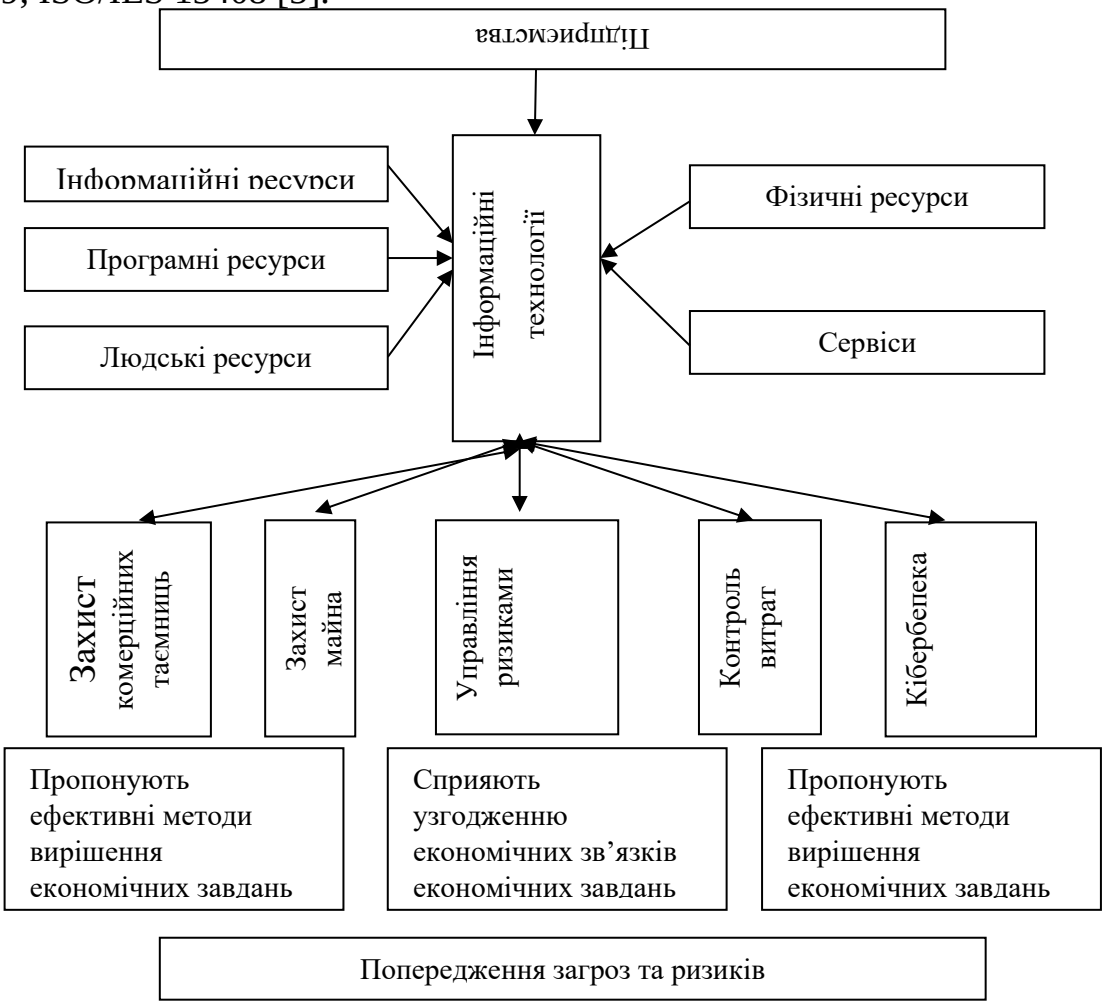

Рис. 1 Структура інформаційної технології управління підприємством. (Розроблено авторами на основі [2-5]).

Модель управління кібербезпекою підприємства можна представити у вигляді двох блоків «загрози бізнес-цінностям підприємства» та «управління ризиками і прийняття рішень, щодо заходів забезпечення кібербезпеки» (рис 2.). Управління кібер-ризиками, як складовою інформаційної безпеки підприємства дозволить:

- погоджувати та контролювати виконання заходів щодо системи інформаційної безпеки;
- запобігти втручанню в інформаційні системи;
- запровадити нові заходи безпеки кіберзагроз, що постійно змінюються та модифікуються.

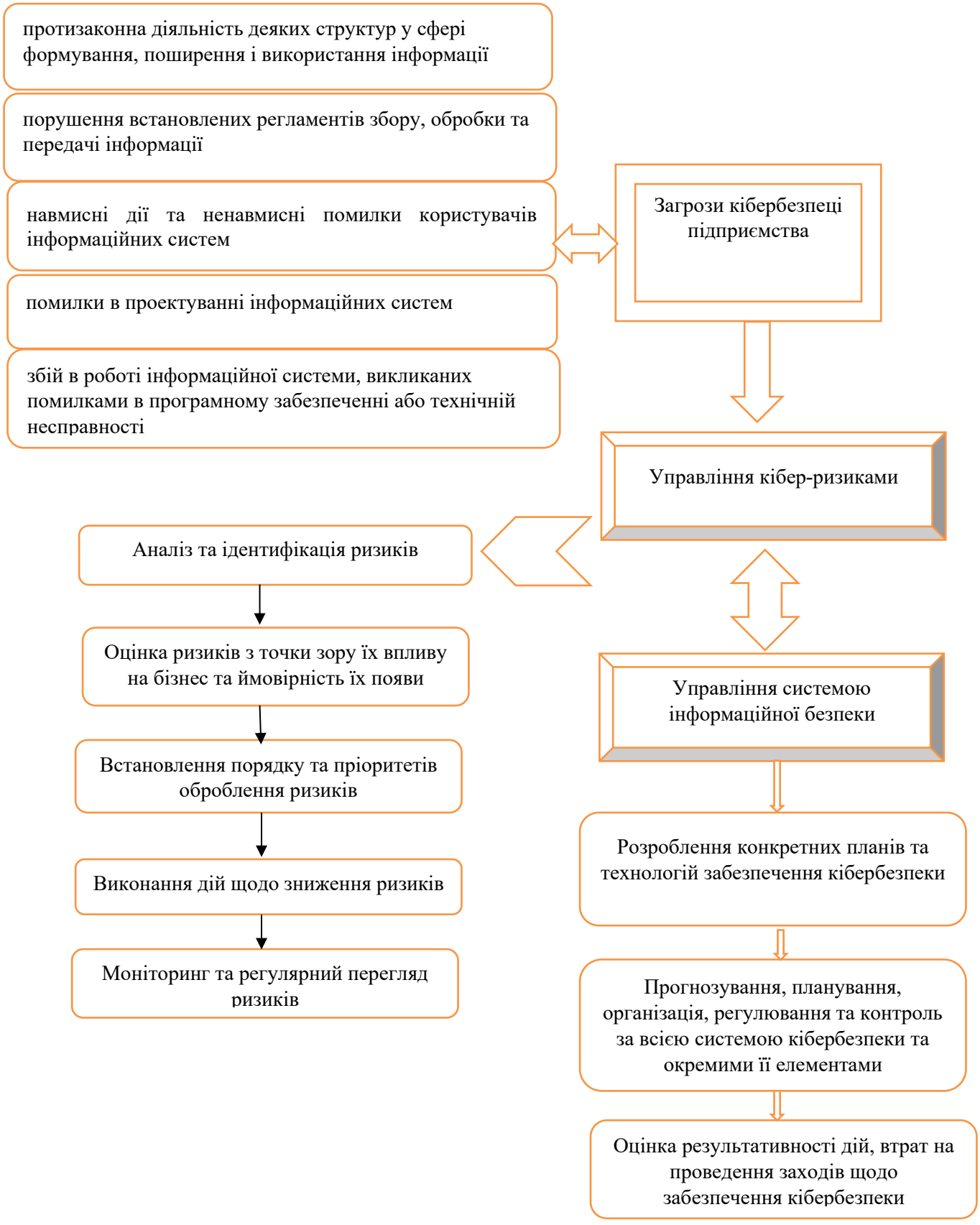

Рис. 2 Модель управління кібербезпекою підприємства.
(Розроблено авторами на основі [2-5]).

Висновки. Впровадження та використання сучасних інформаційних технологій в управління підприємством стає все актуальнішим, а кібербезпека однією зі головних складових економічної безпеки. Як показали дослідження, для забезпечення кібербезпеки доцільно враховувати ризики, які є найкращим засобом контролю та попередження загроз. Моніторинг аналізу ризиків розпочинається з заходів щодо обстеження безпеки інформаційної системи з метою визначення того, які ресурси і від яких загроз потрібно захищати, і наскільки ресурси мають потребу в захисті. Управління кібер-ризиками формується з оцінки розмірів ризиків та створення ефективних методів для зменшення їх масштабів.

Виконання всіх етапів управляння кібербезпекою дозволить виявляти загрози та вразливості інформаційної безпеки підприємства, прорахувати ризики та приймати рішення, успішно управляти інформаційними системами та технологіями.

Список використаних джерел та літератури

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163- VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.05.2023).

2. Онопко А.С., Жигалкевич Ж.М. Застосування інформаційних технологій в управлінні підприємством. URL: https://ela.kpi.ua/bitstream/123456789/22560/1/2017-11_2-18.pdf (дата звернення: 19.05.2023)

3. Інформаційні технології в управлінні організацією: роль, мета та загальна характеристика управлінських IT. URL: https://www.cleverence/articles/auto-busines/informatsionnye-tekhnologii-vupravlenii-organizatsiey-rol-tsel/ (дата звернення: 19.05.2023).

4. Галайко Н.В., Шевченко Н.В. інформаційні технології в управлінні підприємством. *Інформаційні технології в освіті та практиці*: матеріали Науково-практичної конференції (м. Львів, 17 грудня 2021).

5. Огірко І. В. Інформаційні технології та кібербезпека. *Інформаційні технології в освіті та практиці*: матеріали Науково-практичної конференції (м. Львів, 16 грудня 2022).