МОНОГРАФІЯ

СГ НТМ «Новий курс»

НОВИЙ КУРС • WWW.NEWROUTE.ORG.UA
НАНМ УКРАЇНИ • WWW.NEWROUTE.ORG.UA/NANMU
ISCU «PROTON GLOBAL» • WWW.NEWROUTE.ORG.UA/PROTON

ISBN 978-617-7886-93-7
DOI: 10.61718/mon202604

КОНЦЕПТУАЛЬНІ ЗАСАДИ СУЧАСНИХ МІЖДИСЦИПЛІНАРНИХ ДОСЛІДЖЕНЬ

Монографія

Харків • СГ НТМ «Новий курс» • 2026

УДК 001:1
К64

Концептуальні засади сучасних міждисциплінарних досліджень: моногр. – Харків: СГ НТМ «Новий курс», 2026. – 242 с.

ISBN 978-617-7886-93-7
DOI: 10.61718/mon202604

Рецензенти

***Штулер Ірина Юріївна**, доктор економічних наук, професор,*
перший проректор ВНЗ «Національна академія управління»

***Погоріла Світлана Григорівна**, кандидат педагогічних наук,*
доцент кафедри славістичної філології, педагогіки і методики викладання
Білоцерківського національного аграрного університету

***Гетьман Ірина Анатоліївна,** кандидат технічних наук, доцент,*
доцент кафедри комп'ютерних інформаційних технологій
Донбаської державної машинобудівної академії

***Харченко Артем Вікторович**, кандидат історичних наук, доцент,*
доцент кафедри мистецької освіти та гуманітарних дисциплін
Харківського національного університету мистецтв імені І. П. Котляревського

Рекомендовано до друку Вченою радою наукової установи Соціально-гуманітарна науково-творча майстерня «Новий курс» *(протокол № 4мн-2026 від 28.04.2026)*

Видавець СГ НТМ «Новий курс» – діяльність у науковій, видавничій, освітній, творчій, інформаційній сфері з 1989 року. Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 8013 від 22.11.2023. Зареєстровано у Global Register of Publishers. Зареєстровано у Crossref із власним префіксом 10.61718

Монографія буде корисною науковцям, викладачам, здобувачам освіти, а також широкому колу осіб, які цікавляться питаннями розвитку сучасної науки та практики. Монографія оприлюднюється за результатами проведення науково-практичної конференції «Трансформація світу: минуле, сьогодення, майбутнє». За результатами проведення конференції та оприлюднення рукописів автори отримують електронні сертифікати. Сертифікати оприлюднюються на сайті видавця (згідно Порядку підвищення кваліфікації педагогічних і науково-педагогічних працівників, затвердженого постановою Кабінету Міністрів України від 21 серпня 2019 р. № 800).

IV Міжнародна науково-практична конференція (2026)
«Трансформація світу: минуле, сьогодення, майбутнє»

Україна, м. Харків – Румунія, м. Бухарест

26-28 квітня 2026 року

• Освітні науки, педагогіка • Культура, мистецтво • Психологія, соціологія, соціальна робота •
• Фізична культура, спорт • Філософія, релігієзнавство • Філологія, лінгвістика, журналістика •
• Історія, археологія • Економіка, економічна теорія • Підприємництво, торгівля •
• Туризм, готельно-ресторанна справа • Видавнича справа, поліграфія •
• Менеджмент, маркетинг • Державне управління, публічне адміністрування •
• Фінанси, банківська справа, облік, оподаткування • Міжнародні відносини, політологія •
• Право, судова система, правоохоронна діяльність • Воєнні науки, національна та цивільна безпека •
• Інформаційні технології, комп'ютерні науки • Інженерія, виробничі технології •
• Архітектура, будівництво, геодезія • Фізика, хімія, біологія, математика, геологія, екологія •
• Аграрні науки, сільське господарство • Харчові технології, продовольчі системи •
• Ветеринарія, зоотехнія • Охорона здоров'я, медицина, фармація •

ОРГАНІЗАТОРИ

Національна академія наук і мистецтв України
International Scientific-creative Unit «Proton Global»
Соціально-гуманітарна науково-творча майстерня «Новий курс»

www.newroute.org.ua

Зміст

Передмова

Монографія буде корисною науковцям, викладачам, здобувачам освіти, а також широкому колу осіб, які цікавляться питаннями розвитку сучасної науки та практики.

До авторського колективу монографії залучені наступні науковці (інформацію подано мовою оригіналу рукописів): Iryna Bosak, Roksolana Vynnychuk, Supeno Elizabeth, Verbytska Halyna Liubomyrivna, Viktor M. Koryahin, Андреєва Тамара Олександрівна, Боденчук Лілія Борисівна, Бура Тетяна Іванівна, Васильєв Георгій Степанович, Вастьянов Руслан Сергійович, Воробйова Вікторія Іванівна, Горбатюк Оксана Василівна, Гришко Світлана Вікторівна, Джур Ольга Євгенівна, Зав'ялова Тетяна Василівна, Запорожченко Тетяна Петрівна, Зацерковна Роксоляна Станіславівна, Калашніков Валерій Йосипович, Кізь Ольга Богданівна, Коваль Дмитро Олексійович, Коробейнікова Тетяна Іванівна, Куденчук Діана Петрівна, Кучин Сергій Павлович, Ліганенко Ірина Віталіївна, Марутяк Андріяна Андріївна, Матвеєв Сергій Петрович, Мацько Валентина Вікторівна, Мирослава Кадиляк, Мілєва Анастасія Дмитрівна, Непша Олександр Вікторович, Поліщук Світлана Вікторівна, Прохорова Лариса Анатоліївна, Романюк Олександр Никифорович, Савченко Ольга Михайлівна, Стоянов Олександр Миколайович, Ущаповськи Дмитро Юрійович, Хоменко Тетяна Анатоліївна, Ціватий Вячеслав Григорович, Чеботарьова Ганна Михайлівна.

У роботі буде досліджено наступні питання (інформацію подано мовою оригіналу рукописів):

- Творчі й технічні виклики у підготовці репертуарного твору для участі в читецькому конкурсі дистанційного формату;
- Optimisation of basketball players' training activities considering their physical and technical condition;
- Назви автохтонних тварин у німецькій мові;
- Формування математичної компетентності учнів Нової української школи засобом LEGO;
- Формування екологічної культури учнів у процесі навчання географії в умовах Нової української школи;
- Гуманістична парадигма сучасної педагогіки: зміст, принципи та практична реалізація;
- Організаційна культура закладу освіти як чинник гуманізації педагогічної взаємодії;
- Characteristics of human resources management in times of economic instability;
- Features of organizational management of manufacturing enterprises in a turbulent economy and under global challenges;
- Macroeconomic determinants of personnel well-being in the context of economic transformation;
- Венеційська і флорентійська школи дипломатії як центри європейської ідентичності, культури і гуманізму в умовах війн та епідеміологічних криз доби раннього Нового часу (XVI-XVIII ст.): міжнародно-політичний, інституціональний і міждисциплінарний аспекти;
- Вплив корпоративної культури на формування кадрової політики підприємства;
- Економічні важелі мотивації раціонального природокористування та охорони навколишнього природного середовища;
- Науково-технічний розвиток високотехнологічних підприємств: міжнародні тренди розвитку;
- Зародження та становлення економічної освіти Харкова: історичний екскурс;
- Пакування для дитячого харчування: вимоги безпеки та інноваційні рішення;
- Перспективні технології широкоформатного друку: ультрафіолетові, сольвентні, латексні та напрями розвитку галузі;
- Інтегрований підхід до оцінювання та пом'якшення ризиків кібербезпеки організацій з урахуванням ланцюгів постачання програмного забезпечення;
- Адитивні фізичні та електрохімічні методи виробництва, особливості реалізації та перспективи застосування;
- Розроблення дизайну, конструкції та технології виготовлення 3D-картонних пазлів «грай та збирай»;
- Клініко-радіологічна діагностика стенозу хребетного каналу у людей та собак;
- Психологічна готовність майбутніх першокласників до навчання в школі: теоретико-емпіричний вимір.

Інформаційною базою дослідження стали нормативно-правові документи, звіти профільних установ, методичні та статистичні матеріали суб'єктів господарювання, матеріали експертних досліджень, аналітичні огляди, опитування, анкетування, наукові та методичні публікації тощо.

Ключовими критеріями для вибору технології стають економічна ефективність, універсальність матеріалів, екологічна безпечність, енергоефективність та стабільність експлуатаційних характеристик готової продукції. Інтеграція цифрових технологій, автоматизація процесів, розвиток гібридних систем і впровадження нових типів екологічних чорнил відкривають додаткові перспективи для розвитку галузі.

Отже, системний аналіз сучасних технологій друку та інноваційних тенденцій є необхідною передумовою для формування ефективної стратегії розвитку сучасного поліграфічного виробництва, що дозволяє підприємствам залишатися конкурентоспроможними та відповідати вимогам ринку майбутнього.

1. Chepurna K., Khmiliarchuk O., Tkachenko V. *Research into the optical properties of UV inkjet printing on polymeric materials* // «Технологія і техніка друкарства». – 2023. – №3(81). – С. 59-69.
2. Exploring the Future of Best Solvent Inkjet Printers in Industry Trends for 2025. https://www.witcolorprinter.com/blog/future-of-solvent-inkjet-printers-industry-trends-2025/
3. Ультрафіолетовий друк. https://elies.com.ua/ultrafioletovyi-druk/?utm_source=chatgpt.com
4. UV Printing and Why It's Transforming Modern Printing. https://printdigitalsolutions.com/blogs/news/uv-printing-and-why-it-s-transforming-modern-printing?srsltid=AfmBOoqyJmlJEq52UhYi4dyH-mDio6pqkwOWziIc-Q0RU_U4BUCROb15
5. Латексний друк - нова якісна та екологічна технологія. https://www.latexdruk.com.ua/
6. WHAT IS LATEX PRINTING? DEFINITION, PROCESS AND BENEFITS FOR BRANDS. https://www.tissus-print.com/en/blog/printing/technique-innovation/what-is-latex-printing-definition-process-and-benefits-for-brands
7. The Benefits of Latex Printers in 2025: Changing Printing. https://schoolposterprinters.com/the-benefits-of-latex-printers-in-2025-changing-printing/
8. UV, Solvent, Eco-Solvent or Latex? Here's the Real Winner in 2025. https://arrow-digital.com/uv-solvent-eco-solvent-or-latex-heres-the-real-winner-in-2025/

УДК 004.056

Романюк Олександр Никифорович
ORCID: 0000-0002-6497-5056
Доктор технічних наук, професор
Завідувач кафедри програмного забезпечення
Вінницький національний технічний університет
Коробейнікова Тетяна Іванівна
ORCID: 00000000-0003-2487-8742
Кандидат технічних наук, доцент
Доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»
Марутяк Андріяна Андріївна
ORCID: 0009-0007-8567-5996
Студентка
Національний університет «Львівська політехніка»
Куденчук Діана Петрівна
ORCID: 0009-0003-6928-286X
Студентка
Національний університет «Львівська політехніка»

5.3. Інтегрований підхід до оцінювання та пом'якшення ризиків кібербезпеки організацій з урахуванням ланцюгів постачання програмного забезпечення

У роботі запропоновано комплексний підхід до управління ризиками кібербезпеки організацій, який охоплює процеси оцінювання активів, загроз, уразливостей та потенційних втрат. Розглянуто методичні основи ідентифікації та аналізу ризиків у життєвому циклі програмного забезпечення (ПЗ), включаючи етапи розробки, розповсюдження та підтримки. Особливу увагу приділено інтеграції підходів до оцінювання ризиків у контексті ланцюгів постачання технологій кібербезпеки (C-SCRM), що дозволяє враховувати зовнішні фактори впливу та залежності від сторонніх постачальників. Запропоновано структурований метод зменшення ризиків, який включає технічні, організаційні та процесні заходи захисту. Обґрунтовано доцільність використання ризик-орієнтованого підходу, аудиту кібербезпеки та безперервного моніторингу для підвищення стійкості інформаційних систем. Отримані результати можуть бути використані для вдосконалення систем управління кібербезпекою в організаціях різного типу. Ключові слова: кібербезпека, управління ризиками, оцінювання ризиків, активи інформаційних систем, кіберзагрози, аудит кібербезпеки, ланцюги постачання ПЗ, C-SCRM, інформаційна безпека, ризик-орієнтований підхід.

Вступ. В 2021 році міжнародні організації розкрили, що в них відбулось в середньому по 26 інцидентів з безпеки, що більше ніж в 2020 році на 20%. У зв'яку із досить дестабілізованою ситуацією на політичній арені, що відкриває більше дверей хакерам та різноманітним злочинним організаціям, ця цифра буде лише рости. Для

контролю цього ми використовуємо розроблені і стандартні процеси правила та закони для регуляції безпекового аспекту інформаційного простору [1, 2, 3, 4]. Зокрема, у 2022 році 30,000 веб-сайтів було зламано, у 2024 вже 64% компаній мали інциденти з безпеки. Проте спосіб, за допомогою якого злочинці переслідують досягнення своєї мети, залишається єдиним. Це – знаходження вразливостей та їх експлуатація. Тому, такі вразливості в організації мають бути знайдені командою з безпеки до того, як їх експлуатують. Усі вищенаведені аргументи пов'язані із оцінюванням ризиків мережевої безпеки для спеціалізованого підприємства. Тому тема дослідження є *актуальною*.

1. Управління ризиками під час розробки ПЗ та системна інтеграція.

Ризики, пов'язані з якістю ПЗ. Наявність помилок у програмному забезпеченні (ПЗ): помилки можуть призвести до несправносте, зниження продуктивності і втрати даних. ПЗ може не відповідати вимогам організації, що може призвести до необхідності його модифікації. Відсутність документації: відсутність документації може ускладнити використання та підтримку ПЗ.

Ризики, пов'язані з безпекою ПЗ. ПЗ може бути вразливим до атак зловмисників. Використання застарілих технологій може призвести до підвищення вразливості ПЗ до атак. ПЗ може не забезпечувати належного захисту даних, що може призвести до їх витоку або крадіжки.

Ризики, пов'язані з підтримкою ПЗ. Розробник ПЗ може припинити його підтримку, що може ускладнити використання та модифікацію ПЗ.або ж розробник ПЗ може не мати достатніх ресурсів для підтримки ПЗ, що може призвести до затримок у виправленні помилок або впровадженні нових функцій. Для зменшення ризиків, пов'язаних з ПЗ, яке надає стороння організація, можна використовувати ретельний аудит ПЗ і залучення до процесу оцінки ПЗ експертів з безпеки. Закріплення в контракті з розробником ПЗ зобов'язань щодо підтримки ПЗ: це допоможе забезпечити, що ПЗ буде підтримуватися в майбутньому. Оцінка ризиків при оцінці ПЗ, яке надає стороння організація, є важливим етапом, який може допомогти забезпечити якість, безпеку та підтримку ПЗ. Важливо враховувати всі потенційні ризики та розробити ефективні заходи для їх зменшення або усунення.

1.1. Оцінювання загроз і втрат

Оцінювання загроз і втрат – це процес, який дозволяє визначити потенційні кіберзагрози, які можуть вплинути на організацію, а також оцінити потенційні фінансові втрати, які може понести організація в результаті кібератаки.

1) Ідентифікація загроз: тут необхідно визначити всі потенційні кіберзагрози, які можуть вплинути на організацію. Це можна зробити шляхом проведення досліджень, опитування експертів або використання інструментів оцінки загроз.

• Визначення сфери інтересів: необхідно визначити, які активи організації можуть бути зачеплені кібератакою.

• Визначення потенційних загроз: необхідно визначити всі потенційні кіберзагрози, які можуть вплинути на активи, визначені на попередньому підетапі.

2) Оцінка ймовірності реалізації загроз: тут необхідно оцінити ймовірність того, що конкретна загроза буде реалізована. Це можна зробити шляхом використання методів статистичного аналізу або експертних оцінок.

3) Оцінка впливу загроз: тут необхідно оцінити вплив конкретної загрози, якщо вона буде реалізована. Це можна зробити шляхом визначення потенційних фінансових втрат, порушення безпеки або інших негативних наслідків.

Оцінювання втрат:

1) Ідентифікація активів: тут необхідно визначити всі активи організації, які можуть бути пошкоджені або втрачені в результаті кібератаки.

2) Оцінка вартості активів: тут необхідно оцінити вартість кожного активу, який може бути пошкоджений або втрачений в результаті кібератаки. Це можна зробити шляхом використання експертних оцінок.

3) Оцінка ймовірності втрати активів: тут необхідно оцінити ймовірність того, що конкретний актив буде пошкоджений або втрачений в результаті кібератаки. Це можна зробити шляхом використання методів статистичного аналізу.

Заходи для зменшення загроз і втрат. На основі результатів оцінки загроз і втрат можна розробити ефективні заходи для їх зменшення або усунення.

1) Запровадження заходів безпеки можуть допомогти захистити організацію від кібератак. Це може містити використання брандмауерів, антивірусного ПЗ, систем виявлення вторгнень та інших заходів.

2) Персонал організації повинен бути готовий до кібератак. Для цього необхідно проводити навчання з питань безпеки та реагування на кібератаки.

3) Забезпечення резервування: резервування даних і систем може допомогти відновити організацію в разі кібератаки.

Приклади загроз. Зловмисне ПЗ може завдати шкоди або знищити дані, перешкодити роботі систем або красти інформацію. Фішинг – це вид соціальної інженерії, який використовується для обману користувачів увійти в систему на підроблений веб-сайт або надати особисту інформацію. Вторгнення в мережу: вторгнення в мережу – це спроба отримати несанкціонований доступ до мережі організації.

1.2. Оцінювання активів.

Оцінювання активів – це процес, який дозволяє визначити всі активи організації, які можуть бути пошкоджені або втрачені в результаті кібератаки. Це може містити інформацію, обладнання, ПЗ та інші активи.

1) Визначення сфери інтересів: тут необхідно визначити, які активи організації можуть бути зачеплені кібератакою.

2) Ідентифікація активів: тут необхідно визначити активи організації, які можуть бути пошкоджені або втрачені в результаті кібератаки. Це можна зробити шляхом проведення інтерв'ю з персоналом, аналізу документації та аудиту.

3) Оцінка вартості активів – це про вартість кожного активу, який може бути пошкоджений або втрачений в результаті кібератаки. Це можна зробити шляхом використання методів бухгалтерського обліку або експертних оцінок.

Першим кроком у процесі оцінювання активів є визначення сфери інтересів. Це означає визначення, які активи організації можуть бути зачеплені кібератакою. Сфера інтересів може бути визначена на основі наступних факторів: важливість активу для організації, вразливість активу та вплив кібератаки на актив (активи, які можуть завдати найбільшої шкоди організації в разі кібератаки, є найбільш ймовірними цілями для кібератак).

Після визначення сфери інтересів необхідно ідентифікувати всі активи організації, які можуть бути пошкоджені або втрачені в результаті кібератаки шляхом проведення інтерв'ю з персоналом, аналізу документації та проведення аудиту. Інтерв'ю з персоналом можуть допомогти визначити активи, які є важливими для організації та які можуть бути вразливими до кібератак. Аналіз документації визначає активи, які є важливими для організації та які можуть бути вразливими до кібератак. Аудит визначає всі активи організації, які можуть бути пошкоджені або втрачені в результаті кібератаки.

1.3. Оцінка вартості активів.

Оцінка вартості активів є важливим етапом процесу оцінювання активів. Це допомагає визначити, які активи є найбільш ймовірними цілями для кібератак. Вартість активу можна оцінити шляхом використання методів бухгалтерського обліку або експертних оцінок. Метод бухгалтерського обліку передбачає використання вартості, яка відображена в бухгалтерській звітності організації. Експертна оцінка передбачає використання оцінки, яка надана експертом у відповідній галузі.

1.4. Оцінювання загроз.

Оцінювання загроз – це процес, який дозволяє визначити всі потенційні кіберзагрози, які можуть вплинути на організацію. Це містить оцінку ймовірності реалізації загрози та оцінку впливу загрози, якщо вона буде реалізована.

Ідентифікація загроз – визначити всі потенційні кіберзагрози, які можуть вплинути на організацію. Це можна зробити шляхом проведення досліджень, опитування експертів або використання інструментів оцінки загроз.

Оцінка ймовірності реалізації загроз – оцінити ймовірність того, що конкретна загроза буде реалізована. Це можна зробити шляхом використання методів статистичного аналізу або експертних оцінок.

Оцінка впливу загроз – оцінити вплив конкретної загрози, якщо вона буде реалізована. Це можна зробити шляхом визначення потенційних фінансових втрат, порушення безпеки або інших негативних наслідків.

Першим кроком у процесі оцінювання загроз є ідентифікація всіх потенційних кіберзагроз, які можуть вплинути на організацію. Це можна зробити шляхом проведення досліджень, опитування експертів або використання інструментів оцінки загроз. Дослідження можуть допомогти визначити загальні тенденції в кібербезпеці та identifier потенційні загрози, які можуть вплинути на будь-яку організацію. Опитування експертів можуть допомогти identifier загрози, які є найбільш актуальними для конкретної організації. Інструменти оцінки загроз можуть допомогти автоматизувати процес ідентифікації загроз.

Після ідентифікації загроз необхідно оцінити ймовірність того, що конкретна загроза буде реалізована. Це допомагає визначити, які загрози є найбільш важливими для організації. Імовірність реалізації загрози можна оцінити за допомогою методів статистичного аналізу або експертних оцінок. Метод статистичного аналізу передбачає використання даних про попередні кібератаки, щоб визначити, як часто конкретна загроза реалізовувалася в минулому. Експертна оцінка передбачає використання оцінки, яка надана експертом у відповідній галузі.

Оцінка впливу загрози, якщо вона буде реалізована, є важливим етапом процесу оцінювання загроз. Це допомагає визначити, які загрози можуть завдати найбільшої шкоди організації. Вплив загрози можна оцінити шляхом визначення потенційних фінансових втрат, порушення безпеки або інших негативних наслідків. Фінансові втрати можна оцінити шляхом використання методів бухгалтерського обліку або експертних оцінок. Порушення безпеки можна оцінити шляхом визначення потенційних наслідків для операцій організації або конфіденційності інформації. Інші негативні наслідки можна оцінити шляхом визначення потенційних наслідків для репутації організації або її конкурентоспроможності.

1.5. Оцінювання одноразових втрат.

Оцінювання одноразових втрат – це процес, який дозволяє визначити потенційні фінансові втрати, які може понести організація в результаті кібератаки. Це містить оцінку вартості активів, які можуть бути пошкоджені або втрачені в результаті кібератаки. Оцінювання одноразових втрат є важливим процесом, який дозволяє організації оцінити потенційні фінансові втрати, які може понести в результаті кібератаки. За допомогою оцінювання одноразових втрат організація може розробити ефективні заходи для зменшення або усунення цих втрат. Експерти можуть допомогти провести оцінку більш ефективно та точно. Кіберзагрози постійно змінюються, тому важливо регулярно переглядати результати оцінки, щоб врахувати нові загрози.

Результати оцінювання ризиків можуть бути застосовані для розробки ефективних заходів для захисту організації від кібератак. Запровадження заходів безпеки: заходи безпеки можуть допомогти захистити організацію від кібератак. Це може містити використання брандмауерів, антивірусного ПЗ, систем виявлення вторгнень та інших заходів. Персонал організації повинен бути готовий до кібератак. Для цього необхідно проводити навчання персоналу з питань безпеки та реагування на кібератаки.З абезпечення резервування даних і систем може допомогти відновити організацію в разі кібератаки. Результати оцінювання ризиків можуть бути використані для пріоритетизації цих заходів. Це означає, що організації слід зосередитися на першочергових заходах, які можуть допомогти зменшити найбільші ризики.

2. Пом’якшення ризиків.

2.1. Пом'якшення ризиків як процесс.

Пом'якшення ризиків – це процес, який не закінчується після запровадження перших заходів безпеки. Організації повинні регулярно переглядати свої заходи безпеки, щоб забезпечити їх ефективність. Організації також повинні регулярно навчати свій персонал з питань безпеки, щоб персонал був готовий до кібератак.

2.2. Аудит та оцінювання кібербезпеки.

Аудит та оцінювання кібербезпеки – це два важливі процеси, які можуть допомогти організаціям захиститися від кібератак. Аудит кібербезпеки – це незалежний процес, який проводиться для оцінки стану кібербезпеки організації. Аудит може містити перевірку політики безпеки, інфраструктури, ПЗ та персоналу організації. Оцінювання кібербезпеки – це процес, який проводиться для визначення ризиків кібербезпеки, яким схильна організація. Оцінювання може містити аналіз загроз, уразливостей та впливу кібератак.

Аудит кібербезпеки може бути проведений внутрішніми або зовнішніми аудиторами. Внутрішні аудитори є співробітниками організації, які мають знання про її політику безпеки та інфраструктуру. Зовнішні аудитори є незалежними експертами, які мають досвід проведення аудитів кібербезпеки. Аудит кібербезпеки може складатися з:

1. Планування: аудитор визначає цілі аудиту та розробляє план аудиту.
2. Збір даних: аудитор збирає дані про політику безпеки, інфраструктуру, ПЗ та персонал організації.
3. Аналіз даних: аудитор аналізує зібрані дані, щоб визначити ризики кібербезпеки.
4. Звітування: аудитор готує звітність про результати аудиту.
5. Результати аудиту кібербезпеки можуть бути використані для розробки заходів для підвищення кібербезпеки організації.

6. Оцінювання кібербезпеки внутрішніми або зовнішніми експертами. Внутрішні експерти є співробітниками організації, які мають знання про її політику безпеки та інфраструктуру. Зовнішні експерти є незалежними експертами, які мають досвід проведення оцінок кібербезпеки.

7. Ідентифікація активів: оцінювач визначає всі активи організації, які можуть бути пошкоджені або втрачені в результаті кібератаки.

8. Ідентифікація загроз: оцінювач визначає всі потенційні кіберзагрози, яким схильна організація.

9. Оцінка ймовірності загроз: оцінювач оцінює ймовірність того, що конкретна загроза буде реалізована.

10. Оцінка впливу загроз: оцінювач оцінює вплив конкретної загрози, якщо вона буде реалізована.

11. Розрахунок ризиків: оцінювач розраховує ризик для кожного активу, враховуючи його вартість, ймовірність загрози та вплив загрози.

Результати оцінювання кібербезпеки можуть бути використані для розробки заходів для зниження ризиків кібербезпеки. Аудит кібербезпеки та оцінювання кібербезпеки – це два взаємопов'язаних процеси. Аудит може допомогти організації визначити, які ризики кібербезпеки їй необхідно оцінити. Оцінювання – визначити, які заходи необхідні для зниження цих ризиків.

2.3. Підхід до кібербезпеки на основі управління ризиками.

Підхід до кібербезпеки на основі управління ризиками – це методологія, яка використовується для управління кібербезпекою організації. Ця методологія ґрунтується на тому, що всі організації мають кіберризики, і ці ризики необхідно управляти. Підхід до кібербезпеки на основі управління ризиками:

1. Оцінка ризиків містить визначення всіх потенційних кіберзагроз, яким схильна організація, і оцінку ймовірності та впливу цих загроз. Є першим і найважливішим етапом підходу до кібербезпеки на основі управління ризиками і дозволяє організації визначити, які ризики кібербезпеки вона повинна управляти.

2. Управління ризиками містить розробку та впровадження заходів для зниження ризиків кібербезпеки.

3. Контроль ризиків містить регулярний моніторинг кібербезпеки організації, щоб забезпечити ефективність заходів з управління ризиками.

Переваги підходу до кібербезпеки на основі управління ризиками. Підхід до кібербезпеки на основі управління ризиками має переваги: дозволяє організації зосередитися на найважливіших ризиках кібербезпеки; дозволяє організації розробити ефективні заходи з управління ризиками; дозволяє організації регулярно оцінювати ефективність заходів з управління ризиками.

2.4. Управління ризиками та організаційний розвиток.

Управління ризиками та організаційний розвиток – це два взаємопов’язані процеси, які можуть допомогти організаціям досягти своїх цілей. Управління ризиками – це процес, який дозволяє організаціям ідентифікувати, оцінювати та управляти ризиками, які можуть вплинути на їхню діяльність. Організаційний розвиток – це процес, який дозволяє організаціям змінюватися та адаптуватися до нових умов. Управління ризиками може допомогти організаціям зменшити невизначеності, пов’язані з їхньою діяльністю і це може допомогти організаціям приймати більш обґрунтовані рішення та підвищити їхню ефективність; підвищити їхню стійкість до непередбачених подій і це може допомогти організаціям уникнути негативних наслідків ризиків та продовжувати свою діяльність; створювати інновації і це може допомогти організаціям знаходити нові можливості для розвитку та зростання. Управління ризиками є важливим інструментом для організацій, які прагнуть до успіху. Цей інструмент може допомогти організаціям у різних сферах організаційного розвитку, таких як зменшення невизначеності, підвищення стійкості та створення інновацій.

3. Інформаційна технологія управління ризиками ланцюгів постачання технологій кібербезпеки (C-SCRM).

3.1. Технологічний ланцюжок постачання ПЗ (рис. 1):

1) Виробництво: на цьому етапі розробляється ПЗ, тобто мова проектування, розробку, тестування та документацію.

2) Розповсюдження: на цьому етапі ПЗ доставляється користувачам, тобто мова пакування, зберігання, транспортування та продаж.

3) Підтримка: на цьому етапі ПЗ підтримується та оновлюється, тобто йдеться про виправлення помилок, додавання нових функцій та надання технічної підтримки.

Технологічний ланцюжок постачання ПЗ впливає на якість і вартість ПЗ. Якщо технологічний ланцюжок постачання не є ефективним, це може призвести до помилок у програмному забезпеченні, що може вплинути на його надійність і безпеку, водночас призведе до збільшення витрат на розробку, виробництво та розповсюдження ПЗ.

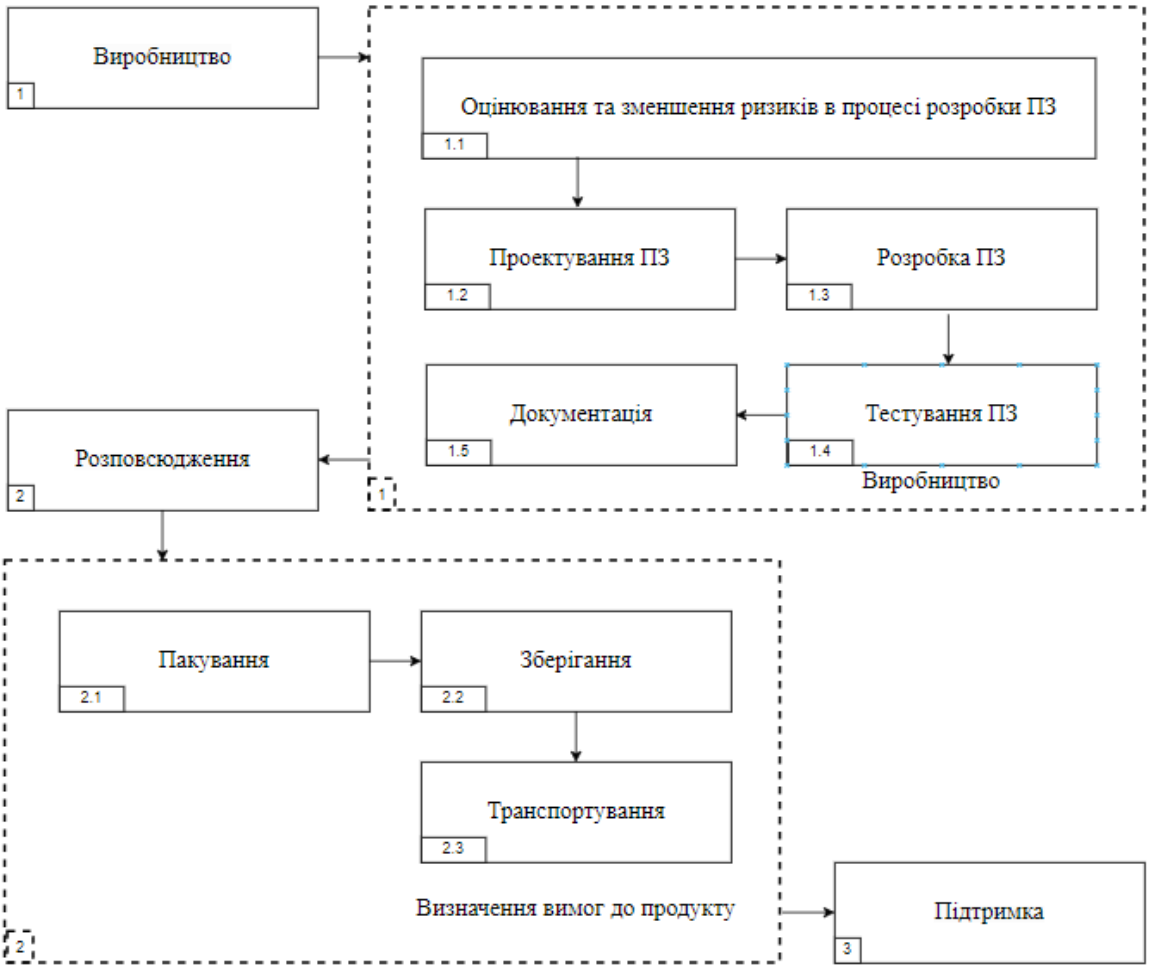

Рис. 1. Технологічний ланцюжок постачання ПЗ

Управління технологічним ланцюжком постачання ПЗ передбачаєтакі завдання:

- Планування – визначаються цілі та завдання управління технологічним ланцюжком постачання.
- Реалізація – реалізуються плани управління технологічним ланцюжком постачання.
- Контроль – контролюється ефективність управління технологічним ланцюжком постачання.

3.2. Процес управління ризиками під час постачання технологій кібербезпеки.

Управління ризиками під час постачання технологій кібербезпеки – це процес, який дозволяє організаціям оцінити та зменшити ризики, пов'язані з придбанням та використанням технологій кібербезпеки. Якщо технології кібербезпеки не будуть безпечними, це може призвести до серйозних наслідків, таких як втрата конфіденційної інформації, фінансові збитки та порушення діяльності.Кроки процесу управління ризиками під час постачання технологій кібербезпеки.

1) Ідентифікація активів. Необхідно ідентифікувати активи, які необхідно захистити. Активами можуть бути конфіденційна інформація, системи, інфраструктура тощо.

2) Оцінка загроз. Необхідно оцінити загрози, які можуть вчинити проти активів. Загрозами можуть бути кібератаки, природні катаклізми тощо.

3) Оцінка уразливостей. Необхідно оцінити уразливості активів, які можуть бути використані для реалізації загроз. Уразливостями можуть бути помилки в програмному забезпеченні, небезпеки в інфраструктурі тощо.

4) Розрахунок ризиків. Необхідно розрахувати ризики для кожного активу, враховуючи його вартість, ймовірність загрози та вплив загрози.

3.3 Метод зменшення ризиків під час постачання ІТ під час розробки ПЗ (рис.2).

Крок 1: Запровадження додаткових заходів безпеки. Запровадження додаткових заходів безпеки: це може включати в себе використання брандмауерів, антивірусного ПЗ, систем виявлення та запобігання вторгненням тощо.

Крок 1.1: Налаштування брандмауерів. Налаштування брандмауера є важливим завданням для будь-якої організації, яка хоче захистити свою мережу.

Крок 1.2: Імплементація антивірусного ПЗ. Антивірусне ПЗ допомагає захистити пристрої та мережі від шкідливого ПЗ, такого як віруси, троянські коні та черв'яки.

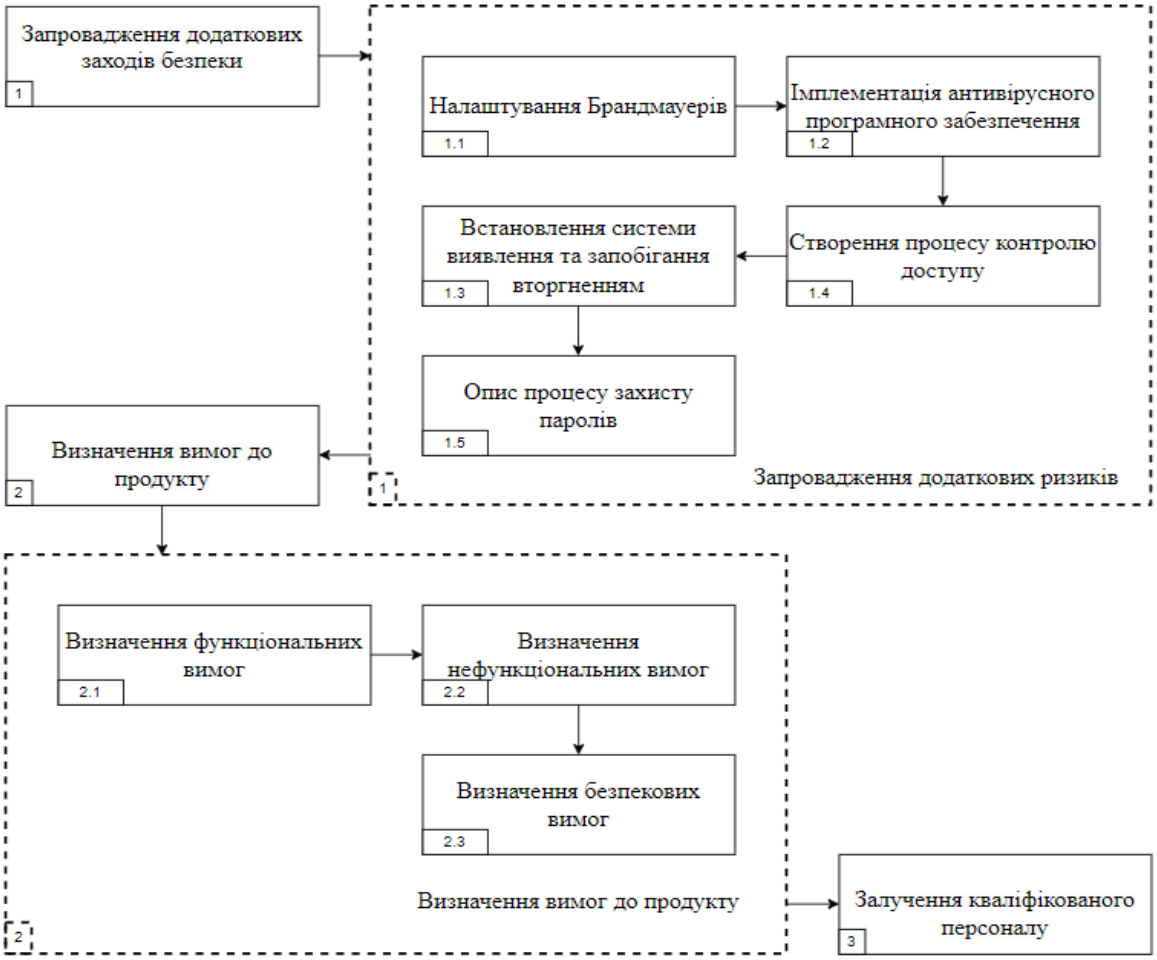

Рис. 2. Метод зменшення ризиків під час постачання ІТ в процесах розробки ПЗ

Крок 1.3: Встановлення систем виявлення та запобігання вторгненням. Воно може бути встановлено на окремих комп'ютерах, маршрутизаторах або на мережному рівні.

Крок 1.4: Опис процесу захисту паролів. Вони використовуються для захисту доступу до ваших облікових записів, таких як електронна пошта, банківські рахунки, соціальні мережі та багато іншого.

Крок 2: Визначення вимог до продукту допоможе уникнути невідповідності продуктів та послуг вимогам замовника.

Крок 2.1: Визначення функціональних вимог допомагає розробникам зрозуміти, що повинна робити система, і гарантують, що система буде відповідати потребам користувачів.

Крок 2.2: Визначення нефункціональних вимог допомагає розробникам зрозуміти, як система повинна працювати, і гарантують, що система буде відповідати потребам користувачів та бізнесу.

Крок 2.3: Визначення безпекових вимог є важливою частиною процесу розробки ПЗ. Вони допомагають розробникам зрозуміти, як захистити систему від кібератак, і гарантують, що система буде відповідати вимогам безпеки бізнесу.

Крок 3: Залучення кваліфікованого персоналу, що може допомогти розробити та впровадити безпечні та якісні продукти та послуги.

Висновки. У результаті проведеного дослідження сформовано узагальнений підхід до оцінювання та пом'якшення ризиків кібербезпеки організацій, який базується на комплексному аналізі активів, загроз, уразливостей та можливих втрат. Встановлено, що ефективне управління ризиками потребує інтеграції процесів оцінювання на всіх етапах життєвого циклу ПЗ, а також урахування факторів ланцюгів постачання технологій кібербезпеки. Обґрунтовано, що використання ризик-орієнтованого підходу дозволяє визначити пріоритетні напрями захисту та оптимізувати розподіл ресурсів організації. Запропонований метод зменшення ризиків, який включає технічні, організаційні та кадрові заходи, забезпечує підвищення рівня захищеності інформаційних систем. Доведено, що регулярне проведення аудиту кібербезпеки, безперервний моніторинг та навчання персоналу є критично важливими для підтримки актуальності захисних механізмів в умовах динамічного розвитку кіберзагроз.

1. Information Security Management System SaaS For ISO 27001 [Ел. ресурс] // Alliantist Ltd. – 2021. – Режим доступу: https://www.isms.online/information-security-management-system-isms/
2. ISO 27001 Requirements – Information Security Management [Ел. ресурс] // Sprinto – 2021. – Режим доступу: https://sprinto.com/blog/iso-27001-requirements/
3. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines [Ел. ресурс] // International Organization for Standardization. – 2019. – Режим доступу: https://www.iso.org/standard/71670.html.
4. Cyber Security: The Onion Approach [Електронний ресурс] – Режим доступу до ресурсу: https://www.jfg-nc.com/cyber-security-the-onion-approach/.
5. T. Korobeinikova, I. Tachenko, R. Chekhmestruk, P. Mykhaylov, O. Romanyuk and S. Romanyuk, "A General Method of Risk Estimation," 2023 13th International Conference on Advanced Computer Information Technologies (ACIT), Wrocław, Poland, 2023, pp. 410-413, doi: 10.1109/ACIT58437.2023.10275626.
6. І. А. Таченко, Т. І. Коробейнікова, С. М. Захаченко Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки // Scientific Collection «InterConf», (84): with the Proc. of the 5th International Scien. and Pract. Conf. «Theory and Practice of Science: Key Aspects». Rome, Italy: Dana, 2021.– С. 417-432.
7. Criticality: A Key Idea in Asset Management [Електронний ресурс] – Режим доступу до ресурсу: https://icma.org/articles/article/criticality-key-idea-asset-management.
8. T. Korobeinikova, I. Tachenko, O. Romanyuk, S. Romanyuk, O. Stakhov and O. Reyda, "Assessing Network Security Risks: a Technological Chain Perspective," 2024 14th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2024, pp. 565-570, doi: 10.1109/ACIT62333.2024.10712586.

DOI: 10.61718/mon202604.06
УДК 621.357

Ущаповськи Дмитро Юрійович
ORCID: 0000-0002-2809-2774
Доцент кафедри технології електрохімічних виробництв
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Воробйова Вікторія Іванівна
ORCID: 0000-0001-7479-9140
Професор кафедри фізичної хімії
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
Васильєв Георгій Степанович
ORCID: 0000-0003-4056-5551
Професор кафедри технології електрохімічних виробництв
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

5.4. Адитивні фізичні та електрохімічні методи виробництва, особливості реалізації та перспективи застосування

Вступ. Адитивні та субтрактивні методи виробництва – це два фундаментально протилежні підходи до створення об'єктів, які сьогодні визначають обличчя сучасної промисловості. *Субтрактивні методи виробництва* – передбачають традиційний підхід, заснований на видаленні зайвого матеріалу з цільної заготовки. Ці методи можуть бути реалізовані за допомогою хімічного (травлення) або механічного (виштамповування, фрезерування, точіння чи свердління) видалення зайвого матеріалу з метою створення потрібного виробу чи деталі. Незважаючи на високі продуктивність, точність та можливість досягнення високого класу чистоти поверхні, основним недоліком цих методів є велика кількість відходів та обмеження у створенні складних внутрішніх порожнин у виробах. Класичними, тобто такими, що стали передумовою до розвитку адитивних методів виробництва можна вважати, наприклад, пресування виробів з порошкових матеріалів, лиття, екструзійні методи, а також

НОВИЙ КУРС • WWW.NEWROUTE.ORG.UA
НАНМ УКРАЇНИ • WWW.NEWROUTE.ORG.UA/NANMU
ISCU «PROTON GLOBAL» • WWW.NEWROUTE.ORG.UA/PROTON

Наукове видання

КОНЦЕПТУАЛЬНІ ЗАСАДИ СУЧАСНИХ МІЖДИСЦИПЛІНАРНИХ ДОСЛІДЖЕНЬ

Монографія

ISBN 978-617-7886-93-7
DOI: 10.61718/mon202604

В межах IV Міднародної науково-практичної конференції (2026)
«Трансформація світу: минуле, сьогодення, майбутнє»
Україна, м. Харків – Румунія, м. Бухарест
26-28 квітня 2026 року

Видання змішаними мовами
Відповідальний секретар – Кучина Т. І.
Формат 60х90 1/8, А4, гарнітура «Times New Roman»
Авторські аркуші – 25,1

ОБИРАЙТЕ ПЕРШИХ!
ДОВІРЯЙТЕ СПРАВЖНІМ!
ЦІНУЙТЕ УНІКАЛЬНІСТЬ!

Видавець СГ НТМ «Новий курс»
Наукова установа
Пр. Перемоги, 77, оф. 179, м. Харків, 61174, Україна
Тел.: +380500301905
Telegram, Viber: +380970440309
www.newroute.org.ua, info@newroute.org.ua

Свідоцтво про внесення суб'єкта видавничої справи до
Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції ДК № 8013 від 22.11.2023
Зареєстровано у Global Register of Publishers
Зареєстровано у Crossref із власним префіксом 10.61718

Приєднуйтесь

Підписка http://surl.li/vvfqkp
Фейсбук-сторінка www.facebook.com/newroute1989
Телеграм https://t.me/newroute1989
Інстаграм www.instagram.com/newroute1989
Вайбер http://surl.li/nbtqz
Фейсбук-група www.facebook.com/groups/secnr

Будемо раді подальшій співпраці!