ОБҐРУНТУВАННЯ

наукової теми

«МЕТОДИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ ПЕРЕРОБКИ ІНФОРМАЦІЇ ТА ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ УПРАВЛІННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Керівник наукової теми: Коршун Н.В., професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, доктор технічних наук, професор

Термін виконання: 06.2022 – 06.2027

Актуальність теми:

Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021, питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління, як національних, так і транснаціональних, формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів. Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій.

З початком повномасштабного вторгнення РФ проблеми забезпечення інформаційної безпеки стали ще більш актуальними. На початку 2022 року країна-агресор почала нарощувати інтенсивність кібератак проти українських організацій та для підтримки стратегічних і тактичних цілей російських військ. Ці дії мають на меті у тому числі порушити доступ до інформації та критично важливих послуг, від яких залежить життя цивільного населення, а також похитнути довіру до керівництва країни.

Зі звітів за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку видно, що кількість атак значно зросла, при цьому у 2022 році 65% підозрілих подій виявлені у міністерствах та організаціях.

Значне зростання кількості атак у порівнянні з 4 кварталом 2021 року фіксує Avast: кількість троянських атак віддаленого доступу - більш ніж на 50%, атак зловмисного програмного забезпечення - більш ніж на 20% «у країнах, які беруть участь у війні». 10guards повідомляє, що у порівнянні з аналогічним періодом 2021 року кількість DDoS-атак була в 4,5 рази більшою, при цьому спостерігалася безпрецедентна тривалість DDoS-сесій, зокрема на інтернет-ресурси банків та держструктур.

Дослідження Microsoft свідчить про те, що Росія об’єднує ракетні удари з кібератаками по Україні для завдання більшої шкоди інфраструктурі.

Результатом кібератак є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування об’єктів критичної інфраструктури, які безпосередньо впливають на стан національної безпеки і оборони.

Проблеми забезпечення інформаційної безпеки на критично важливих об'єктах, з огляду на появу нових та зростання рівня існуючих ризиків і загроз в інформаційному просторі України, набувають великої значущості і потребують відповідного наукового підґрунтя для їх вирішення.

Сучасні науково-практичні напрацювання в Україні, а так само ряд провідних міжнародних стандартів містять норми й вимоги, спрямовані в основному на захист від несанкціонованого доступу. При цьому вони часто не забезпечують базового рівня безпеки, тому що дозволяють моделювати лише частину загроз. При цьому в даний момент не існує загальноприйнятих стандартів або підходів, що дозволяють забезпечити підвищений або високий рівень захисту. Так само до негативного боку застосування сучасних стандартів варто віднести шаблонність пропонованого захисту й відсутність варіантності.

Враховуючи зазначене вище, питання забезпечення інформаційної безпеки інформаційних систем переробки інформації та програмно-технічних комплексів управління критичної інфраструктури є актуальним та потребує подальшого аналізу, вивчення та вдосконалення.

Об’єкт дослідження: інформаційні системи переробки інформації та програмно-технічні комплекси управління критичної інфраструктури.

Предмет дослідження: методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури в умовах зростання потужності кібератак та ймовірності цільового ураження систем.

Мета дослідження: забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури в умовах впливу інформаційних загроз, ризиків і невизначеностей.

Завдання дослідження:

- визначити ступінь важливості інформаційних об’єктів критичної інфраструктури для безпеки держави;
- проаналізувати основні інформаційні загрози, ризики і невизначеності для інформаційних систем переробки інформації та програмно-технічних комплексів управління критичної інфраструктури;
- розробити методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури в умовах впливу інформаційних загроз, ризиків і невизначеностей.

Очікувана теоретична та практична значущість дослідження:

1) **на теоретико-методологічному рівні**:

- аналіз інформаційних загроз, ризиків в умовах невизначеності у рамках забезпечення безпеки комунікаційних систем та системи управління технологічними процесами об’єктів критичної інфраструктури держави;
- опрацювання ключових термінів і понять в галузі функціональної та кібербезпеки програмно-технічних систем критичного застосування;
- розробка методики віднесення об’єктів інфраструктури до критично важливих;
- розробка методів та моделей забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки.

2) **на рівні практичного впровадження**:

- надання практичних рекомендацій щодо впровадження сучасних технологій у виробничу практику органам державної влади та установам, що відносяться до критично важливих об'єктів інформатизації, з метою підвищення рівня захищеності цих об'єктів;
- розроблення та використання в освітньому процесі кафедри робочих програм нових навчальних дисциплін для різних рівнів вищої освіти; електронних навчальних ресурсів; спеціалізованих курсів для

викладачів в рамках підвищення кваліфікації; оновлення змістового наповнення існуючих дисциплін;

- створення платформ для постійної взаємодії наукової спільноти та фахівців-практиків галузі, зокрема, через організацію та проведення міжнародних науково-практичних конференцій, науково-практичних семінарів для науковців і викладачів, студентських конференцій, форумів та інших заходів.

Результати дослідження будуть:

- узагальнені й опубліковані у традиційному форматі наукових статей, колективної монографії, довідкових та навчально-методичних матеріалів;
- представлені у форматі електронних навчальних ресурсів;
- апробовані на міжнародних і всеукраїнських конференціях, форумах, з'їздах, круглих столах, науково-практичних семінарах.

Результати дослідження можуть стати основою для формування теоретико-методологічних засад забезпечення функціональної та кібербезпеки інформаційних систем переробки інформації та програмно-технічних систем критичного застосування в умовах впливу інформаційних загроз, ризиків і невизначеностей.

ПЛАН РЕАЛІЗАЦІЇ НАУКОВОЇ ТЕМИ

Етап / Назва дослідження	Очікувані результати		Очікувані наукові продукти (статті, монографії тощо)	Дата виконання
	на теоретичному рівні	на практичному рівні		
Організаційний/ аналітичний	Вивчення та узагальнення світового досвіду забезпечення інформаційної безпеки критично важливих об'єктів. Опрацювання ключових термінів і понять в галузі функціональної та кібербезпеки програмно-технічних систем критичного застосування.	Встановлення та розвиток зв'язків з організаціями, установами, підприємст-вами задля спільної розробки наукової теми, вивчення та використання передового наукового досвіду.	Наукові статті, тези, матеріали конференцій тощо.	06.2022-11.2023
Дослідницький	Розробка методики віднесення об'єктів інфраструктури до критично важливих. Обґрунтування та розроблення методів та моделей забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури.	Оновлення змісту освітньо-професійних програм, робочих програм навчальних дисциплін, електронних навчальних ресурсів; створення спеціалізованих курсів в рамках підвищення кваліфікації.	Наукові статті, тези, матеріали конференцій, навчально-методичні матеріали тощо	12.2023-02.2026
Узагальнюючий	Розробка практичних рекомендацій для органів державної влади та установ, що відносяться до критично важливих об'єктів інформатизації з метою підвищення рівня їх захищеності	Підвищення рівня захищеності критично важливих об'єктів інформатизації в результаті імплементації результатів дослідження.	Підсумковий звіт, наукові статті, тези, проєкти технічної документації, проєкти постанов органів влади, колективна монографія.	03.2026-06.2027