Міністерство освіти і науки України
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»
Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

Білостоцький технологічний університет (Польща)

Університет прикладних наук (Литва)

Відземський університет прикладних наук (Латвія)

Університет «Aurel Vlaicu» в м. Арад (Румунія)

Міжнародний науково-освітній та навчальний центр (Естонія)

Київський національний університет імені Тараса Шевченка
Кафедра фінансів

Донецький національний університет імені Василя Стуса

Національний технічний університет «Дніпровська політехніка»

Луцький національний технічний університет

Одеський національний економічний університет

РОЗВИТОК ФІНАНСОВОГО РИНКУ В УКРАЇНІ: ЗАГРОЗИ, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Матеріали VII Міжнародної науково-практичної конференції

27 листопада 2025 р.

Полтава
2025

УДК 336.58:004.056.5

***Кудінова Аліна Олександрівна*[4],**
кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

КІБЕРЗАХИСТ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ УКРАЇНИ

У сучасних умовах повномасштабної військової агресії кібербезпека набуває критичного значення для забезпечення фінансової безпеки України. Кібератаки ворога є невід'ємною частиною гібридної війни, спрямованою на дестабілізацію критичної інфраструктури (банківський, енергетичний, транспортний сектори), підрив довіри до державних інституцій та уповільнення економічних процесів. Стійкість національної системи до кіберзагроз стає ключовим фактором, що визначає здатність держави функціонувати, захищати активи та забезпечувати майбутню відбудову.

Ефективність національної системи кіберзахисту критично залежить від швидкості обміну інформацією про потенційні та актуальні загрози. В Україні вже функціонує модель оперативного сповіщення бізнесу та держструктур, що дозволяє компаніям вживати превентивних заходів. В умовах постійних кібератак роль держави виходить за межі простого технічного захисту, виконуючи три взаємопов'язані стратегічні функції [3]:

Нормативно-правове та стратегічне регулювання – створення чіткої правової бази (гармонізація з Директивою NIS2), визначення стандартів та обов'язків для критичної інфраструктури, а також встановлення юридичної відповідальності за кіберзлочини [2].

Оперативне реагування та координація – забезпечення роботи 24/7, що включає моніторинг кіберпростору (Threat Intelligence), інформування та оперативне оповіщення бізнесу, координацію дій у кризових ситуаціях (Держспецзв'язку, СБУ) та розслідування кіберінцидентів.

Освітня, просвітницька та кадрова діяльність, яка спрямована на підвищення «кібергігієни» суспільства та створення кадрового резерву (проведення кампаній, інтеграція курсів із кібербезпеки, формування кібервійськ та резерву) [4].

Для формування ефективної системи раннього виявлення атак важливе впровадження сучасних технічних та інноваційних рішень:

– використання SIEM-систем (Security Information and Event Management) для відслідковування підозрілої активності в реальному часі;

– застосування можливостей штучного інтелекту (ШІ) для аналізу мережевого трафіку, виявлення аномалій та прогнозування атак;

– перенесення даних у захищені хмарні середовища міжнародних компаній (Amazon AWS, Microsoft Azure, Google Cloud), що підвищило стійкість критичних державних реєстрів у 2022 році.

Компаніям, що працюють у критичних секторах (банківський, енергетичний тощо), рекомендовано запроваджувати базові правила кібергігієни, крім того, важливим є впровадження ключових технічних компонентів кіберзахисту, що охоплюють мережевий рівень, захист кінцевих точок, вебзастосунків та корпоративної пошти [5].

На рівні пересічного користувача кібергігієна формує «кіберщит» суспільства. Дотримання простих правил (використання складних паролів, регулярне оновлення, розпізнавання фішингу, використання VPN) знижує ефективність ворожих атак. Масова цифрова грамотність також є ключовим завданням.

[4] Тези підготовлено в межах виконання НДР молодих учених «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди», державний реєстраційний номер 0124U000615

Таблиця 1

Технічні компоненти кіберзахисту [1]

Компонент	Опис
AntiDDoS protection	Захист від атак типу відмови в обслуговуванні.
Web Application Firewall	Захист корпоративних вебзастосунків та API від атак типу OWASP.
Email Security & Antispam	Захист корпоративної пошти від фішингу та шкідливих вкладень.
Next Generation Firewall	Захист на мережевому рівні, фільтрація корпоративного трафіку.
Endpoint Protection	Захист кінцевих точок від відомих атак та атак нульового дня.
UBA & UEBA	Захист робочого простору та контроль на базі ШІ.
Network Access Control	Захист доступу до корпоративної мережі від неавторизованих користувачів.

Повноцінна економічна відбудова України, відновлення інфраструктури та залучення інвестицій неможливі без забезпечення високого рівня кіберстійкості. У повоєнний час необхідно:

1. Інституціоналізувати національний кіберрезерв на основі створення системи підготовлених фахівців (за зразком естонської Cyber Defence League) з числа волонтерів та IT-фахівців для оперативного залучення у випадку масованих атак.
2. Створити розгалужену мережу галузевих центрів реагування, розширити функціонал CERT-UA, створивши галузеві центри (у фінансовому секторі, енергетиці, транспортній логістиці тощо) як оперативні та аналітичні осередки.
3. Масове підвищення цифрової грамотності через інтеграцію курсів з кібергігієни у шкільну та університетську програми, розробляти національні освітні кампанії для дорослого населення.
4. Стимулювати розвиток кіберекосистеми – підтримати створення національної освітньої програми (на прикладі американської CyberCorps) для підготовки тисяч професійних експертів у галузі інформаційної безпеки.

Отже, в умовах воєнного стану в Україні сформувалася стійка система кіберзахисту, посилена міжнародною підтримкою та інноваційними технічними рішеннями. Однак, для забезпечення довгострокової фінансової безпеки та успішної відбудови необхідно трансформувати технічний захист у культуру кіберстійкості, що вимагає поєднання стратегічного державного регулювання, просунутих технологій, кваліфікованого кадрового резерву та масової цифрової грамотності суспільства і бізнесу. Кіберзахист має стати не просто функцією спеціалістів, а невід'ємною частиною повсякденних практик.

Література

1. Cybersecurity Framework. National Institute of Standards and Technology (NIST). URL: https://www.nist.gov/cyberframework.
2. Директива (ЄС) 2022/2555 Європейського Парламенту і Ради від 14 грудня 2022 р. про заходи для забезпечення високого спільного рівня кібербезпеки в усьому Союзі (Директива NIS2). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
3. Звіти та аналітика щодо кіберзахисту. Міністерство цифрової трансформації України. Офіційний вебсайт. URL: https://thedigital.gov.ua.
4. Кіберзагрози та економічна безпека: сценарії для України : аналітична доповідь. Український інститут майбутнього. Київ, 2023.
5. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки.* 2024. 2(49). 307-313. https://doi.org/10.32782/2308-1988/2024-49-49
6. Онищенко С.В., Маслій О.А. Ризики та загрози в умовах цифровізації: безпековий аспект. II International 223 Scientific Conference Development of Socio-Economic Systems in a Global Competitive Environment: Conference Proceedings, May 24th, 2019. Le Mans, France. P.54-56.