ГОЛУБ ІВАН
Інститут професійної освіти НАПН України (м. Київ)

КІБЕРЗАХИСТ ДІЯЛЬНОСТІ НАУКОВИХ УСТАНОВ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ

Актуальність теми зумовлена стрімким зростанням кіберзагроз, що особливо посилилися після повномасштабного вторгнення росії в Україну. Упродовж 2022–2025 років країна зазнала численних кібератак, які суттєво підвищили вимоги до кіберстійкості державних установ, у тому числі й наукових. Наукові установи НАПН України акумулюють та обробляють значні обсяги інтелектуальної власності, результати досліджень, персональні дані науковців і освітню аналітику. Водночас їхній кіберзахист часто має фрагментарний характер і недостатньо врегульований нормативно.

Провівши аналіз поточного стану кіберзахисту установ НАПН України, ми розробили комплекс науково обґрунтованих рекомендацій та адаптивну модель його вдосконалення.

Наукова новизна полягає у першому комплексному дослідженні кіберзахисту наукових установ НАПН України в умовах війни. Виявлено типові вразливості з урахуванням гуманітарного профілю цих установ, розроблено адаптивну модель, що враховує обмеженість ресурсів, та запропоновано шляхи реалізації системного підходу.

Проведений аналіз теоретико-методологічних засад дав змогу чітко розмежувати поняття: «кібербезпека» як ширший концепт проактивної діяльності та «кіберзахист» як сукупність практичних заходів. Досліджено специфіку кіберзахисту наукових установ, де основними активами є результати досліджень, інтелектуальна власність, персональні дані та освітні платформи.

Розглянуто міжнародний досвід (США, Велика Британія, Нідерланди, Німеччина) та стандартів кібербезпеки, зокрема ISO/IEC 27001, NIST CSF, Zero Trust Architecture і рекомендацій ENISA. Порівняння українського та європейського нормативного забезпечення (наприклад, GDPR) показало активну інтеграцію України в європейський кіберпростір, однак також виявило потребу в адаптації й деталізації цих норм до національних реалій.

Емпірична частина дослідження охопила опитування 30 наукових співробітників. Жоден із них не підтвердив наявність внутрішньої політики кібербезпеки, понад половина взагалі не знали про її існування. Лише 3,3 % респондентів регулярно створювали резервні копії документів, тоді як 70 % не проходили жодного навчання з кібербезпеки за кошт установи.

Виявлені проблеми включають:

– організаційну фрагментацію – відсутність єдиної політики та координації між інститутами;

– кадровий дефіцит – відсутність спеціалістів з кібербезпеки й недостатній рівень кваліфікації ІТ-фахівців;

– слабкий технічний захист – обмежене використання 2FA, нерегулярне резервне копіювання, відсутність IDS/IPS та систем шифрування даних;

– невизначене фінансування – заходи з кіберзахисту не передбачені окремими бюджетними статтями.

Найпоширенішими кіберзагрозами для установ НАПН України є фішинг, компрометація електронної пошти, DDoS-атаки на сайти, несанкціонований доступ до архівів та дезінформаційні кампанії. Переважна більшість інцидентів зумовлена людським фактором та відсутністю цілісної політики кіберзахисту.

Запропонована модель кіберзахисту для установ НАПН України ґрунтується на гібридному підході, що поєднує міжнародні стандарти з урахуванням національних потреб та обмежених ресурсів. Передбачено її поетапне впровадження у 2025–2027 рр.:

1. Організаційні заходи – розробка уніфікованої політики інформаційної безпеки, призначення відповідальних у кожній установі, щорічні тренінги з кібергігієни, створення планів реагування на інциденти.

2. Технічні заходи – централізований антивірусний захист, системи резервного копіювання (на основі open-source рішень), 2FA, SSL-сертифікати, оновлення CMS та вебзастосунків, базовий мережевий моніторинг.

3. Кадрове забезпечення – розробка типової посадової інструкції для відповідального з кібербезпеки, безперервний розвиток кіберкомпетентностей через вебінари, розсилки, тестування знань.

4. Міжвідомча взаємодія – створення єдиного центру координації кіберзахисту НАПН України, стандартизація звітності про інциденти, співпраця з CERT-UA, Держспецзв'язку, СБУ та Кібер-поліцією для обміну інформацією про загрози.

Очікуваний ефект від впровадження моделі – зменшення кількості кіберінцидентів на 30–50 % у перший рік, формування культури кібербезпеки та забезпечення довгострокової кіберстійкості.

Практичне значення дослідження полягає у можливості використання результатів керівництвом НАПН України та її структурними підрозділами для побудови ефективних систем кіберзахисту, розроблення внутрішніх політик, впровадження технічних рішень та підвищення обізнаності персоналу.

Отже, кіберзахист наукових установ НАПН України є критично важливим елементом національної безпеки. Проведений аналіз виявив низку системних проблем: відсутність внутрішніх політик, кадровий і технічний дефіцит, недостатнє фінансування та організаційну фрагментацію. Водночас розроблена адаптивна модель, що базується на міжнародних стандартах та враховує національні реалії, відкриває шляхи до якісного вдосконалення захисту інформаційних активів. Її впровадження дозволить знизити кількість кіберінцидентів, сформувати культуру безпечного поводження з даними та забезпечити стійкість роботи наукових установ у сучасних умовах.

Література

1. Держспецзв'язку. (10 листоп. 2022). Кількість кібератак на Україну продовжує зростати. ArmyInform. https://surl.li/buuool

2. Закон України «Про критичну інфраструктуру» № 1882-IX від 16 листопада 2021 року. (2022). Відомості Верховної Ради України, 7, ст. 48. https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. (2018). Відомості Верховної Ради України, 5, ст. 36. https://surl.li/ywdvnl

4. Рада національної безпеки і оборони України. (2021). Проєкт Стратегії кібербезпеки України (14 с.). https://surl.li/eyxmwu

ДУЖИЙ РОМАН
Національний університет оборони України (м. Київ)

ВИЗНАЧЕННЯ ЗМІСТУ КОМПЕТЕНТНОСТЕЙ ВІЙСЬКОВОСЛУЖБОВЦІВ ЗСУ ДЛЯ УСПІШНОГО ВИКОНАННЯ ЗАВДАНЬ В МІЖНАРОДНИХ ОПЕРАЦІЯХ З ПІДТРИМАННЯ МИРУ І БЕЗПЕКИ

Одним із важливих складових формування зовнішньої політики України та посилення політичних зв'язків з НАТО, ООН та ЄС є залучення військовослужбовців Збройних Сил України (далі – ЗСУ), які пройшли курсову підготовку, до міжнародної діяльності щодо встановлення миру та безпеки у світі шляхом направлення національного контингенту, національного персоналу та матеріально-технічних ресурсів і послуг у розпорядження відповідних органів.

Згідно із ст. 6 Закону України «Про участь України в міжнародних операціях з підтримання миру і безпеки» [1] (із змінами) громадяни України, які включаються до складу національного контин-генту або направляються для участі в міжнародній операції з підтримання миру і безпеки як національ-ний персонал, попередньо проходять спеціальну підготовку у відповідних учбових, спеціальних цент-рах або у визначених органах військового управління, військових частинах (підрозділах). В нинішніх реаліях створення моделі системи курсової підготовки військовослужбовців для участі в МОПМБ, правильне визначення компетентностей, які повинні набути військовослужбовці по завершенню курсової підготовки, забезпечать змогу у майбутньому досягти високої ефективності навчання, підвищать її якість та скоротять витрати і час на підготовку.

Визначення дефініцій компетентностей є ключовим для створення системи курсової підготовки військовослужбовців для участі в МОПМБ, тому спершу їх необхідно сформулювати. Чітке формулювання повинно забезпечити:

– відповідність міжнародним стандартам. МОПМБ проводяться під егідою ООН, НАТО чи інших міжнародних організацій. Компетентності випускників курсів повинні відповідати вимогам міжнародного гуманітарного права, стандартам організацій, що координують такі операції;

– підвищення якості підготовки. Необхідно адаптувати курсову підготовку до актуальних викликів, наприклад, роботи у багатонаціональних командах, реагування на кризові ситуації чи використання сучасних технологій моніторингу. Це підвищує ефективність навчального процесу та забезпечує готовність військовослужбовців до виконання завдань за призначенням;

– забезпечення взаємодії в багатонаціональних підрозділах. МОПМБ передбачають взаємодію між військовими, поліцейськими і цивільними з різних країн. Потрібні гарантії, що військовослужбовці матимуть уніфіковані навички і знання, необхідні для командної роботи в міжнародному контексті;

– фокус на міжкультурну комунікацію та етику. Участь у миротворчих операціях вимагає особливої чутливості до культурних, релігійних і соціальних особливостей регіону [2]. Необхідно інтегрувати ці аспекти в курсову підготовку, що мінімізує ризик непорозумінь і конфліктів;