Co-funded by the Erasmus+ Programme of the European Union

# РОЗВИТОК ЦИФРОВОЇ ГРАМОТНОСТІ МАЙБУТНІХ ПРАВООХОРОНЦІВ ДЛЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

**Лунгол Ольга,**
к.пед.н., доцент, доцентка кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3,
Донецький державний університет внутрішніх справ, м. Кропивницький, Україна
ORCID: https://orcid.org/0000-0001-8128-0072

Гібридні загрози є одним із найважливіших викликів для національної безпеки у сучасному світі і особливо актуальні для України в умовах повномасштабного вторгнення. Гібридні загрози характеризуються використанням як традиційних, так і новітніх інструментів та методів впливу, серед яких інформаційні та кіберзагрози займають центральне місце. У зв'язку з цим, підготовка майбутніх правоохоронців має включати розвиток їх цифрової грамотності, що є необхідною умовою для ефективної протидії сучасним викликам.

Цифрова грамотність – це здатність використовувати цифрові технології для пошуку, аналізу, оцінювання та використання інформації. Сєров Ю. та Бобришева П. включають в цифрову грамотність три поняття: медіаграмотність, інформаційна грамотність, технологічна грамотність [1, с. 209] та зазначають, що навички розпізнавати неправдиву інформацію, перевіряти джерела та порівнювати інформацію або факти є критично важливим та надійним інструментом у грамотному використанні медіа, як у професійній діяльності, так і в особистих цілях. В контексті протидії гібридним загрозам цифрова грамотність включає в себе знання про основні принципи роботи цифрових систем, розуміння механізмів інформаційної безпеки та вміння працювати з великими масивами даних. Зростання кібератак, дезінформації та маніпуляцій вимагає від майбутніх правоохоронців здатності ідентифікувати, аналізувати та нейтралізувати ці загрози. Таким чином, цифрова грамотність стає важливою компетенцією, яка в загальному комплексі забезпечуватиме готовність курсантів до протидії гібридним загрозам[2].

Для формування цифрової грамотності майбутніх правоохоронців необхідно застосовувати комплексний підхід, що включає: теоретичне вивчення основ кібербезпеки, практичні заняття з використанням спеціалізованого програмного забезпечення, навчання використанню технологій OSINT (Open Source Intelligence), роботу з симуляційними моделями та тренажерами, розвиток критичного мислення та медіаграмотності. В комплексі, курсанти мають оволодіти основами роботи цифрових систем, знати принципи захисту інформації, види кіберзагроз та методи протидії їм, працювати з інструментами для аналізу даних, з виявлення кібератак та

проведення цифрового розслідування тощо. Опанування методів збору та аналізу інформації з відкритих джерел сприятиме розвитку аналітичного мислення та вміння працювати з великими обсягами даних, що є важливим у боротьбі з інформаційними загрозами. Оскільки дезінформація є невід'ємною частиною гібридних загроз, курсанти мають навчитися розрізняти фейкову інформацію та критично оцінювати отримані дані.

На сьогоднішній день існує ряд прикладів успішної реалізації програм з розвитку цифрової грамотності в закладах освіти, які здійснюють підготовку майбутніх правоохоронців. Наприклад, впровадження спеціалізованих курсів з кібербезпеки, створення навчальних лабораторій з аналізу цифрових даних та проведення практичних занять із застосуванням технологій OSINT. Також значного поширення набули тренінги з протидії інформаційним загрозам, які включають у себе розгляд конкретних кейсів, що відображають реальні загрози, з якими стикаються правоохоронці у своїй діяльності.

Особливої уваги заслуговує використання онлайн-курсів та освітніх серіалів, які пропонують практичні знання та навички у сфері інформаційної та кібербезпеки. Такі курси допомагають формувати необхідні компетентності майбутніх правоохоронців і забезпечують доступ до актуальної інформації та методик протидії гібридним загрозам. Онлайн-курси, що розміщені на платформі Дія. Освіта (наприклад, «Кібергігієна для молоді», «Базові знання з кібегігієни», «Кібергігієна: як захиститися від фішингу», «Школа OSINT», «Аналітик із кібербезпеки», «Як захиститися від фейків та дезінформації», «Персональна кібергігієна» тощо) дозволяють курсантам отримати базові знання про кіберзагрози, навчитися ефективно захищати себе від фішингу та дезінформації, а також здобути практичні навички роботи з інструментами OSINT. Ці знання є фундаментальними для формування інформаційної та кібербезпекової компетентностей.На платформі Prometheus курсанти можуть пройти курси, такі як «Безпека в інтернеті під час війни: практичний курс», «Цифрова безпека на персональному рівні»,«Цифрова безпека для громадських організацій в умовах війни» та ін. Ці матеріали допоможуть зрозуміти специфіку кіберзагроз у військовий час, навчитися працювати з персональними даними та використовувати практичні засоби захисту в мережі Інтернет. На платформі EdEra доступні курси «Захист персональних даних», «Години медіаграмотності», «Фактчек: довіряй-перевіряй» тощо, які сприяють розвитку критичного мислення, навичок перевірки фактів та основ медіаграмотності. Вміння перевіряти інформацію та відрізняти правдиві дані від фейкових є однією з ключових компетенцій для правоохоронців у боротьбі з гібридними загрозами.

Додатково, актуальні рекомендації та практичні поради щодо кіберзахисту курсанти можуть опрацювати на сайтах Департаменту кіберполіції України [3] та Державної служби спеціального зв'язку та захисту інформації України [4]. Зазначені ресурси містять практичні приклади з реальних

розслідувань та матеріали, що дозволяють майбутнім правоохоронцям дізнатися про найновіші тенденції у сфері кібербезпеки.

З педагогічної точки зору, інтеграція таких ресурсів в освітній процес сприяє розвитку самостійного навчання, підвищенню мотивації курсантів та забезпечує актуальність освітніх матеріалів. Онлайн-курси дозволяють адаптувати процес навчання під індивідуальні потреби курсантів, що є важливим у підготовці майбутніх фахівців правоохоронної галузі. Також використання платформ дистанційного навчання сприяє розвитку компетентностей з управління власним часом і ресурсами, що є важливими для майбутньої професійної діяльності.

Отже, цифрова грамотність є ключовою компетенцією для майбутніх правоохоронців, яка дозволяє ефективно протидіяти гібридним загрозам. Розвиток цієї навички вимагає комплексного та систематичного підходу, що включає теоретичну підготовку, практичні заняття, використання сучасних технологій та розвиток критичного мислення. Інтеграція таких методів у процес підготовки правоохоронців сприятиме підвищенню ефективності їхньої роботи в умовах сучасних викликів безпеці.

**Список використаних джерел:**

1. Сєров Ю., Бобришева П. Цифрова грамотність: критичне мислення та аналіз інформації в Інтернеті. 2024. С. 209 – 210.
2. Лунгол О. Удосконалення професійної підготовки майбутніх фахівців правоохоронної діяльності засобами інформаційних технологій. *Наука і техніка сьогодні*. № 7(7). 2022. С. 152 – 162.
3. Сайт кіберполіції України. Рекомендації. URL: https://cyberpolice.gov.ua/articles/ (Дата звернення: 28.09.2024).
4. Сайт Державної служби спеціального зв’язку та захисту інформації України. URL: https://cip.gov.ua/ua/faqs(Дата звернення: 28.09.2024).