припинення дезінформації є ключовими складовими етичної політичної поведінки в цифровій ері.

Вирішення цих питань вимагає комплексного підходу, який включає в себе розробку та вдосконалення законодавства, активну участь соціальних мереж у захисті прав користувачів та навіть залучення міжнародних організацій для розробки стандартів безпеки в цій сфері

1. Токарєва К. Забезпечення інформаційних прав людини в соціальних мережах Актуальні проблеми правознавства. 4 (32)/2022 DOI :10.35774/app2022.04.088

2. Вірна Ж. П. Інформаційні права і свобода в структурі правового статусу сучасної людини. Особистісне зростання: теорія і практика: зб. наук. праць IV Міжнар. наук.-практ. Інтернет-конф. (м. Житомир, 21 квітня 2020 р.). Житомир, 2020. С. 210–213.

СИНИЦІНА Юлія
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

АКТУАЛЬНІ ПИТАННЯ ПІДГОТОВКИ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОРГАНІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сучасному етапі розвитку України інформаційні технології набули поширення в усіх сферах людської діяльності. Виникла й стрімко розвивається потужна індустрія отримання, систематизації та поширення інформації. Кількість працівників в інформаційному секторі у більшості країн світу до яких відноситься й Україна неухильно збільшується. Інформація набуває значення одного з найбільш затребуваних державних ресурсів.

Суттєві зміни відбуваються і в діяльності правоохоронних органів. Зокрема на основі інформаційних технологій упроваджуються потужні інформаційно-пошукові системи, удосконалюється система управління та інформаційно-аналітичного забезпечення Національної поліції, розробляються нові методи збирання й аналізу інформації, розширюються можливості спеціальних технічних засобів тощо. Водночас сучасними інформаційними технологіями оснащується й кримінальне середовище [1].

Проблемі формування моделі фахівця присвячено дослідження І.Д. Беха, І. А. Зязюна, Г.В. Єльникової, Л.В. Козак, А.К. Маркової, О.І. Мармази, О.О. Романовського, В.А. Семиченко, С.О. Сисоєвої, О.М. Спіріна, Н.Ф. Тализіної, В.В. Ягупова та інших науковців. Окремі аспекти

підготовки фахівців у галузі інформаційних технологій для правоохоронних органів розглядалися в наукових працях С.І. Апухтіна, О.М. Бандурки, О.М. Барановської, В.В. Бачила, В.О. Голубєва, В.Є. Козлова, В.А. Кудінова, Г.Ю. Маклакова, А.С. Овчинського, Ю Ю. Орлова, В.Л. Ортинського, В.Д. Поливанюка, та інших науковців.

Актуальні питання підготовки фахівців у галузі інформаційних технологій для органів національної поліції України включають ряд важливих аспектів:

1. Кібербезпека та кіберзахист:

– Організація тренінгів з кібербезпеки для ефективного захисту інформаційних систем поліції від кібератак.

– Розробка та впровадження політик кіберзахисту для запобігання витокам конфіденційної інформації.

Забезпечення кібербезпеки поліції – пріоритетна задача. Організація тренінгів у сфері кібербезпеки дозволяє підвищити навички фахівців та ефективно захищати інформаційні системи від кібератак. Розробка та впровадження політик кіберзахисту визначає рамки для запобігання витокам конфіденційної інформації, забезпечуючи надійний захист важливих даних та дотримання стандартів безпеки.

2. Комп'ютерна криміналістика:

– Навчання фахівців сучасним методам дослідження комп'ютерних злочинів та цифрового доказування.

– Підготовка до розслідування електронних слідів інтернет-злочинів.

Навчання фахівців у галузі комп'ютерної криміналістики включає ознайомлення із сучасними методами дослідження комп'ютерних злочинів та навичками цифрового доказування. Спеціалісти отримують знання для ефективного розслідування електронних слідів інтернет-злочинів, що стає дуже важливим у сучасній цифровій ері, де кіберзлочини стають все поширенішими. Таке навчання сприяє вдосконаленню методів виявлення та протидії комп'ютерній злочинності [2].

3. Аналіз використання великих баз даних:

– Вивчення методів та інструментів аналізу великих обсягів даних для виявлення закономірностей та трендів у кримінальній діяльності.

– Забезпечення навичок роботи з аналітичними платформами.

Навчання аналізу використання великих баз даних включає вивчення методів та інструментів для виявлення закономірностей та трендів у кримінальній діяльності. Фахівці отримують навички роботи з аналітичними платформами, що дозволяє їм ефективно обробляти та інтерпретувати великі обсяги даних. Це допомагає виявляти ключові відомості та сприяє більш ефективному розслідуванню кримінальних подій через використання сучасних технологій аналізу.

4. Електронне слідство:

– ***Навчання ефективному збору та аналізу електронних доказів у судових справах.***

– ***Застосування сучасних методів для виявлення та вивчення цифрових слідів.***

Навчання електронного слідства передбачає отримання навичок ефективного збору та аналізу електронних доказів у судових справах. Спеціалісти вивчають сучасні методи для виявлення та вивчення цифрових слідів, що є важливим у контексті розслідувань кримінальних подій. Використання новітніх технологій у сфері електронного слідства сприяє об'єктивному та ефективному процесу здобуття та представлення доказової бази у судових процедурах.

5. Захист від кіберзагроз:

– ***Організація навчань щодо виявлення та протидії кіберзагрозам, які можуть впливати на діяльність поліції.***

– ***Постійне оновлення захисних заходів та політик безпеки інформаційних систем.***

Захист від кіберзагроз включає організацію навчань, спрямованих на виявлення та протидію потенційним кіберзагрозам, які можуть впливати на діяльність поліції. Фахівці отримують необхідні навички для ефективної реакції на кібератаки. Постійне оновлення захисних заходів та політик безпеки інформаційних систем є важливим елементом стратегії, що гарантує високий рівень кібербезпеки та надійність функціонування поліцейських інформаційних структур.

6. Етичні аспекти використання технологій:

– ***Поглиблення знань щодо етичних норм використання технологій у роботі правоохоронних органів.***

– ***Розробка стандартів та директив, які враховують етичні вимоги до застосування новітніх технологій у роботі поліції.***

Зосередження на етичних аспектах використання технологій у сфері правоохоронних органів є ключовим завданням. Навчання фахівців стосовно етичних норм використання технологій у роботі правоохоронців допомагає поглибити їхні знання та визначити етичні межі застосування новітніх засобів. Розробка стандартів і директив, які враховують етичні вимоги, є необхідною для забезпечення відповідального та прозорого використання технологій у діяльності поліції.

Навчання фахівців у сфері інформаційних технологій для національної поліції важливо спрямоване на забезпечення ефективного використання сучасних інструментів у боротьбі з кримінальністю та забезпечення безпеки громадян.

---

1. Анісімов К.І. Сутність та значення концепції «community policing» у діяльності органів національної поліції України Правовий часопис Донбасу № 3 (76) 2021. DOI : https://doi.org/10.32366/2523-4269-2021-76-3-169-174

2. Синиціна Ю.П., Прокопов С.О., Рижков Е.В. Спеціальна техніка в правоохоронній діяльності Навч. посібн. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 244 с. URL : https://er.dduvs.in.ua/handle/123456789/8735

ГАЙВАНЮК Іветта
курсантка 1 курсу
ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
РИЖКОВ Едуард
ппрофесор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ІНФОРМАЦІЙНА ТА ЕКОНОМІЧНА БЕЗПЕКА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Основою національної безпеки є економічна безпека. Вона охоплює у себе фінансові ресурси України, людські ресурси та усю економічну систему в цілому. Інформаційна безпека, в свою чергу, захищає кіберпростір нашої держави. Економічна безпека включає в себе охорону економіки на національному та на міжнародному рівнях, тому є досить важливою складовою держави. Інформаційні технології, які використовуються задля вироблення, обробки та передавання інформації, зокрема, мають забезпечувати економічну безпеку України. До них належить опрацювання та надійне зберігання інформації, яка знаходиться в усіх інформаційних системах. Для подібних дій потрібне обов'язкове залучення технологій, таких, як сервери, сховища даних та надійне програмне забезпечення.

Забезпечення економічної та інформаційної безпеки відбувається за допомогою кіберзахисту, кібергігієни, аналітики даних, шифрування даних, моніторингу, їх надійних баз та ін. Акценти воєнної боротьби зміщуються в бік практичної реалізації інформаційних технологій [1]. Тому наразі коли на території України триває війна, інформаційна та економічна безпека мають бути основними питаннями, що мають бути розглянуті державою, адже інформаційний простір – це також зброя.

Захист інформаційних даних в Україні має бути надійним та комплексним для охорони систем даних, особливо під час війни. Військовий стан зараз дає змогу розвитку кіберзахищенності держави саме у військовій сфері. Збройні сили України, з моменту повномасштабного вторгнення