Базиленко Альона Сергіївна
курсант 204 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

СИСТЕМА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Зазначене є яскравим прикладом відомої парадигми «Хто володіє інформацією, той володіє світом».

Сучасне суспільство стикається з серйозними викликами у сфері правопорядку та безпеки, що породжені зростанням злочинності, спричиненим різноманітними соціальними та економічними факторами. Недостатня взаємодія та обмін інформацією між правоохоронними органами може призвести до неефективності у виявленні злочинів та притягненні винних до відповідальності. Для подолання цих проблем невід'ємною є впровадження та постійне вдосконалення інформаційних технологій у правоохоронній сфері.

На законодавчому рівні, інформаційне забезпечення органів поліції – це комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на поліцію завдань. Інформаційні підсистеми як складові системи інформаційного забезпечення призначені для збирання, накопичення, зберігання та обробки інформації з певних напрямів обліків і орієнтовані на використання в діяльності більшості правоохоронних структур, мають загальний характер і належать до загальновідомчих інформаційних систем [1].

Наприклад, на думку В.А. Кудінова та К.В. Ярового під сучасними інформаційними технологіями слід розуміти сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації в інтересах її користувачів [2, с. 119].

Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» (далі – ІПНП) – це сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції та її інформаційно-аналітичного забезпечення.

Крім цього, до основних завдань системи ІПНП слід віднести:

- інформаційно-аналітичне забезпечення діяльності Національної поліції України;
- забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС;
- забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу;
- забезпечення електронної взаємодії з МВС та іншими органами державної влади [3].

Забезпечення доступу до надійної та актуальної інформації для правоохоронних органів, співпраця між ними на національному та міжнародному рівнях, а також використання передових технологій інформаційної безпеки є важливими складовими ефективної системи правоохоронного заходу. Розвиток інформаційних технологій та постійне удосконалення процесів обробки та аналізу даних мають визначальне значення для підвищення ефективності правоохоронної діяльності та забезпечення гармонійного розвитку суспільства [2, с. 106]. Проте важливо відзначити, що процес збору та обробки даних має охоплювати всі аспекти діяльності компонентів Національної поліцейської системи, які визначені законодавством України.

Створення та оптимізація цифрових платформ для обміну даними, таких як бази даних та інформаційні системи, може суттєво полегшити співпрацю між правоохоронними органами. Розробка та впровадження програмного забезпечення для аналізу великих обсягів даних дозволить ефективно виявляти та прогнозувати тенденції злочинності. Крім цього, забезпечення адекватного рівня кібербезпеки для захисту цих інформаційних систем від кібератак є необхідною умовою боротьби зі злочинністю в онлайн-середовищі. Такі заходи сприятимуть забезпеченню безпеки громадян і підвищенню ефективності правоохоронної діяльності.

На нашу думку питання вдосконалення інформаційного забезпечення правоохоронних органів набуває особливої актуальності. Дуже важливими характеристиками зібраної інформації має бути повнота, достовірність, доступність, актуальність, точність. Це може стати чи не головним чинником, який сприяє діяльності поліції, адже в умовах розвитку висока якість інформаційного забезпечення правоохоронних органів є запорукою їхньої ефективної діяльності, а отже покращенням стану захисту прав і свобод людини і громадянина в нашій державі.

Список використаних джерел:

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради. 2015. № 40-41. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
2. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.
3. Наказ МВС України від 03.08.2017 № 676 (зареєстровано в Міністерстві юстиції України 28 серпня 2017 р. за № 1059/30927) «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»». URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

Бехтер Ростислав Олександрович
курсант 206 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

АНАЛІЗ ПРОБЛЕМ КІБЕРБУЛІНГУ ТА ОНЛАЙН-ПЕРЕСЛІДУВАННЯ В УМОВАХ ВОЄННОГО СТАНУ

У зв’язку з воєнним станом, проблема кібербулінгу та онлайн-переслідування набуває особливого значення. Це важливе явище, яке може поглибити соціальні та психологічні напруження в суспільстві та серед військовослужбовців. Кібербулінг, як і офлайн булінг, може призвести до серйозних наслідків для жертв, зокрема до стресу, депресії та інших психічних проблем. Онлайн-переслідування може стати інструментом для дестабілізації та дискредитації ворожих сил. На передовій це може викликати додаткові труднощі для військових, зокрема збільшити їх вразливість та відволікання від виконання бойових завдань. Для вирішення цих проблем необхідно розробити комплексні стратегії кібербезпеки, включаючи навчання персоналу, використання захисту даних та моніторингу соціальних мереж. Такі заходи допоможуть зменшити вплив кіберагресії на військовий контекст та забезпечити безпеку та захист учасників конфлікту.

Проблематика кібербулінгу та засоби протидії йому представляють новий напрямок для наукового дослідження на сьогодні, оскільки поки що не проводилися глибокі наукові дослідження з цієї теми.