

Рева Сергій Миколайович

*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*

АКТУАЛЬНІ ПРОБЛЕМИ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УМОВАХ ВОЄННОГО СТАНУ

Зустрічаючи сучасну динаміку конфліктів та зміни політичного ландшафту, інформаційні технології стають ключовим фактором у веденні військових операцій та забезпеченні національної безпеки. В умовах воєнного стану вони набувають ще більшого значення та актуальності, створюючи як виклики, так і можливості для сучасних армій та керівництва країни. У цьому контексті важливо розглянути низку ключових проблем, що виникають у зв'язку з використанням інформаційних технологій у воєнному середовищі, а також шляхи їх вирішення та можливі наслідки для суспільства та безпеки нашої країни.

Захисту інформації приділяють увагу багато вчених як в Україні, так і за кордоном. Особливо гостро на сьогодні, з урахуванням умов постійної конкуренції не лише між недержавними структурами, а і структурами, які містять державні інформаційні ресурси, точиться боротьба за інформацію. Тому її захист завжди актуальний. Актуальні питання сучасних інформаційних технологій досліджували такі фахівці, як В. М. Богуш, М. В. Грайворонський, О. А. Довидьков, В. Г. Кривуца, В. Ф. Шаньгин, О. Г. Корченко, Г. Ф. Конахович, В. Г. Грибунін та інші вчені. Таким чином, метою зазначеної роботи є удосконалення науково-методичного апарату оцінювання ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів національної поліції.

Єдина конкурентна перевага, яку має наша країна в цьому аспекті, це традиційно сильні ІТ-кадри, тобто в Україні дуже високий рівень підготовки програмістів. 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 наочним підтвердженням загальновідомої тези «хто володіє інформацією, той володіє світом» [1, с. 202].

Слід зазначити, що 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 [2, с. 67].

Звичайно в даній темі є свої проблемні питання кібербезпека, воєнний стан ускладнює облаштування та захист інформаційних систем. Напади на важливі мережі, військові бази та комунікаційні канали можуть призвести до розколу комунікацій та перешкоджати стратегічним операціям. Досягнення захисту інформаційних технологій здійснюватиметься шляхом ужиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підлив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективною системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки [3, с. 117].

Сучасні інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації в інтересах її користувачів. Види сучасних інформаційних технологій: - інформаційна технологія опрацювання даних; - інформаційна технологія керування; - інформаційна технологія підтримки прийняття рішень; - інформаційна технологія експертних систем [4, с. 396-397].

Наприклад, на нашу думку основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є:

- удосконалення форм та методів управління системами інформаційного забезпечення;
- централізація та інтеграція комп'ютерних банків даних;
- впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків;
- розбудова та широке використання ефективних та потужних комп'ютерних мереж;
- застосування спеціалізованих засобів захисту інформації;
- налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні [5, с. 72].

Враховуючи вищевикладене слід зазначити, що сьогоденні воєнні реалії чітко демонструють, що інформація є зброєю «масового ураження». Тому необхідно створити ефективний механізм, який би забезпечив державну інформаційну безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію. Найбільша цінність українців полягає у їх розумінні та сприйнятті понять свобода і справедливість. Саме це вони зараз відстоюють, і розплачуються за них власним життям. Для побудови ефективної системи інформаційної безпеки важливо покласти в його основу три логічні складові механізму цієї системи:

1) технічна – тобто створення і функціонування всіх необхідних технічних складових систем;

2) політична – державна політика повинна бути спрямована на забезпечення інформаційної безпеки;

3) правова – оформлення всіх пов'язаних елементів у якісні нормативно-правові акти.

Таким чином, формування інформаційної безпеки в умовах війни є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини. У час війни публічно-правовий захист виходить за межі традиційного регулювання і поглинає приватно-правові відносини. Необхідно розуміти, що за умов воєнних дій держава часто об'єктивно неспроможна гарантувати права людини в повному об'ємі. Однак збереження фундаментальних засад на основі політичної та правової взаємодії механізмів забезпечення інформаційної безпеки оберігає підвалини демократії та систему загальних принципів права від руйнування волонтаристськими рішеннями. Якщо війна валить стіни нашої конституційної оселі – міцний фундамент демократизму дасть змогу їх відновити і відбудувати.

Список використаних джерел:

1. Танкушина Т. Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність // Вісник Запорізького національного університету: збірник наукових праць.

2. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

3. Про новий підхід до взаємодії поліції з населенням на основі сучасних інформаційних технологій // «Сучасні проблеми правового, економічного та соціального розвитку держави»: тези доп. V Міжнародної науково-практичної конференції (м. Харків, 18 листопада 2016 року) / МВС України, Харківський національний університет внутрішніх справ. – Харків, 2016. – 472 с.

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n14>.

5. Крайнов В. О., Маланчук М. Ф., Грозовський Р. І. Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління. К.: НУОУ, Сучасні інформаційні технології у сфері безпеки та оборони, 2020р. № 1(37). С. 103-106.

Самойленко Олександра Віталіївна
курсант 201 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 МЕХАНІЗМІВ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ

У зв'язку із значним прогресом технологій та інформаційних систем, соціальні мережі знаходять широке застосування у різних сферах людської діяльності, включаючи бізнес, політику та правоохоронну сферу. Актуальним питання сьогодення є протидія дезінформації у кіберпросторі. У сучасному світі поширення інформації стало незаперечним ключовим фактором, що значно впливає на формування громадської думки та утримання суспільства в напрузі, особливо в умовах конфлікту чи війни.

Аналіз останніх досліджень і публікацій за обраною темою свідчить, що теоретичні та практичні аспекти пов'язані з питаннями інформаційної безпеки були предметом численних досліджень. Зокрема, слід окремо відзначити наукові роботи таких вчених, як: Корнейка О.В., Корчевського М.В., Кудінова В.А., Хахановського В.Г., Ярового К.В. та інших. Проте, порушене питання потребує подальшого дослідження з метою розробки новітніх нормативно-правових підходів для ефективною протидії дезінформації у соціальних мережах, особливо в умовах воєнного стану.

З початку 2013 року в Україні активно почали звертати увагу на проблему дезінформації. Особливу увагу приділено «сучасним інформаційним війнам», де не лише проаналізовано суть та витоки інформаційного конфлікту, але й детально вивчено зміни в інформаційному просторі під час інформаційного протистояння.