МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій

та кібербезпеки ННІ № 1

Присвячується
35-річчю кафедри інформаційних технологій та кібербезпеки

МАТЕРІАЛИ

міжвідомчого науково-практичного круглого столу на тему:

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ»

(*м. Київ, НАВС, 25 квітня 2024 року*)

Київ – 2024

УДК 343.9:004.7 (477)
ББК Ю
К 887

Матеріали круглого столу за загальною редакцією:

Кудінов В.А. – професор кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ, кандидат фізико-математичних наук, доцент;

Яровий К.В. – старший викладач кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ, кандидат юридичних наук.

Рецензенти:

Звєрєв В.П. – заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату РНБО України, кандидат технічних наук, старший науковий співробітник;

Хахановський В.Г. – професор кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ, доктор юридичних наук, професор.

Матеріали обговорено, схвалено та рекомендовано до друку на засіданні кафедри інформаційних технологій та кібербезпеки ННІ № 1 (протокол № 22 від 10 травня 2024 року), Вченої ради ННІ № 1 Національної академії внутрішніх справ (протокол № 5 від 13 травня 2024 року).

Всі матеріали надані в авторській редакції та виражають персональну позицію учасників круглого столу

К887 **Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану**: матеріали міжвідомчого науково-практичного круглого столу (м. Київ, НАВС, 25 квітня 2024 р.); за заг. редакцією В. А. Кудінова, К. В. Ярового. К.: Нац. акад. внутр. справ, 2024. 144 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжвідомчий науково-практичний круглий стіл на тему: «Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану», який відбувся на базі кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ 25 квітня 2024 року.

Призначені для курсантів, студентів та слухачів, а також науково–педагогічних працівників закладів вищої освіти системи МВС України.

Можуть бути корисними для слухачів магістратури, докторантури та аспірантури, наукових та практичних працівників органів та підрозділів МВС України, Національної поліції України.

ББК Ю

ЗМІСТ

ІСТОРІЯ СТАНОВЛЕННЯ КАФЕДРИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ ННІ № 1 НАВС

Історія становлення кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС містить цікавий та насичений різними подіями шлях, який безпосередньо пов'язаний з історією становлення провідного закладу вищої освіти системи Міністерства внутрішніх справ – Національної академії внутрішніх справ.

ДАТА	***НАЗВА КАФЕДРИ***	
25.06.1988	кафедра технічних засобів попередження та розкриття злочинів	Київської вищої школи МВС СРСР ім. Ф.Е. Дзержинського
01.05.1990	кафедра інформаційно-обчислювальної техніки	
01.09.1991	кафедра технічних засобів попередження та розкриття злочинів	
27.01.1992	кафедра технічних засобів попередження та розкриття злочинів	Української академії внутрішніх справ
10.01.1996	кафедра оперативної техніки	
20.12.1996	кафедра оперативної техніки	Національної академії внутрішніх справ України
30.08.1999	кафедра інформаційних технологій	Інституту підготовки управлінських кадрів НАВС України
21.07.2000		Інституту управління НАВС України
15.01.2003		НАВС України
08.09.2005		Київського національного університету внутрішніх справ
27.08.2010		НАВС
19.07.2013		навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції НАВС
07.11.2015		навчально-наукового інституту № 1 НАВС
01.09.2017	кафедра інформаційних технологій та кібернетичної безпеки	навчально-наукового інституту № 1 НАВС
17.10.2018 – дотепер	кафедра інформаційних технологій та кібербезпеки	

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Навчально-науковий інститут № 1
Кафедра інформаційних технологій та кібербезпеки

П Р О Г Р А М А

проведення міжвідомчого науково-практичного круглого столу на тему:

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ»

(*25 квітня 2024 року*)

Київ – 2024

Дата проведення: **25 квітня 2024 року**

Початок роботи: 15.00

Місце проведення: *Національна академія внутрішніх справ (м. Київ, пл. Солом'янська 1, змішаний формат: очно – зал педагогічної майстерності; дистанційно – з використанням платформи для організації відеоконференцій ZOOM).*

Регламент: доповіді – *до 5 хв.*, обговорення – *до 3 хв.*

Відкриває захід завідувач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, кандидат технічних наук, професор **Корнейко О.В.**

Вступне слово модератора заходу, старшого викладача кафедри інформаційних технологій та кібербезпеки ННІ № 1, Голови ради молодих вчених НАВС, кандидата юридичних наук **Ярового К.В.**

ДОПОВІДІ:

1. Начальник 4-го управління (оперативно-аналітичного забезпечення та аналізу відкритих джерел) Департаменту кіберполіції НПУ **Панченко Є.В.** «Аналітика кластерів зі збору коштів на допомогу російській армії, що пов'язані з віртуальними активами».

2. Начальник Територіального управління БЕБ у м. Києві **Драгунов В.В.** «Посилення аналітичної функції БЕБ».

3. Старший інспектор 9-го відділу (оперативного пошуку та партнерства у сфері інформаційних технологій) Управління протидії кіберзлочинів в м. Києві **Чепур І.М.** «Шляхи протидії дезінформації на прикладі інформаційного простору BRAMA».

4. Радник Ірпінського міського голови, Голова Ірпінської молодіжної ради, заступник Голови обласної молодіжної ради, підприємець **Андрущенко Д.І.** «Впровадження інноваційних технологій в умовах воєнного стану на прикладі міста-герой Ірпінь (Click City)».

5. Доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки ДонДУВС, Голова наукового товариства ДонДУВС, доктор філософії **Габорець О.А.** «OSINT: a scientific approach to informed decision-making».

6. Старший науковий співробітник науково-дослідної лабораторії з проблемних питань кримінального аналізу, викладач кафедри кібербезпеки та інформаційного забезпечення, Голова ради молодих вчених ОДУВС, кандидат юридичних наук, адвокат **Биков І.О.** «Антикорупційний вплив відкритих даних».

7. Курсант 204 н. гр. ННІ № 3 НАВС **Базиленко А.С.** «Система інформаційного забезпечення Національної поліції України» (к.ю.н. Яровий К.В.).

8. Курсант 204 н. гр. ННІ № 3 НАВС **Бойчура М.Ю.** «Проблеми інформаційного забезпечення України в умовах воєнного стану» (к.ю.н. Яровий К.В.).

9. Курсант 2 курсу факультету № 4 ХНУВС **Борисова К.Є.** «Потенціал використання інформаційних технологій (ШІ) для оптимізації надання домедичної допомоги поліцейським» (к.т.н. Світличний В.А.).

10. Ад'юнкт кафедри криміналістики та судової медицини НАВС **Васюта Ю.В.** «Розслідування кіберзлочинності спільними слідчими групами крізь призму криміналістичних інновацій».

11. Курсант 201 н. гр. ННІ № 3 НАВС **Вишневська М.Ю.** «Сучасний стан кіберзахисту України в умовах повномасштабної війни» (к.ю.н. Яровий К.В.).

12. Курсант 204 н. гр. ННІ № 3 НАВС **Войцеховська Д.М.** «Стан дослідження питання інформаційного забезпечення Національної поліції України» (к.ю.н. Яровий К.В.).

13. Курсант 2 курсу факультету № 4 ХНУВС **Глущенко І.О.** «Деякі особливості використання технологій штучного інтелекту в діяльності поліції України» (к.т.н. Світличний В.А.).

14. Курсант 208 н. гр. ННІ № 1 НАВС **Головко О.В.**, старший науковий співробітник наукової лабораторії з проблем протидії злочинності ННІ №1 НАВС, кандидат юридичних наук **Ботнаренко І.А.** «Аспекти та питання кібербезпеки для України в умовах воєнного стану».

15. Студентка 102 БПМС н. гр. ННІ № 1 НАВС **Грянко А.Г.** «Аналіз проблем інформаційного забезпечення у ході воєнного часу» (к.ю.н. Яровий К.В.).

16. Студент 102 БПМС н. гр. ННІ № 1 НАВС **Драченко З.Д.** «Сучасні технології захисту інформації в умовах сьогодення» (к.ю.н. Яровий К.В.).

17. Курсант 204 н. гр. ННІ № 3 НАВС **Дубова А.П.** «Питання протидії дезінформації у мережі Інтернет в умовах воєнного стану» (к.ю.н. Яровий К.В.).

18. Курсант 2 курсу факультету № 4 ХНУВС **Жмуровська К.Р.** «Вплив дезінформації на громадську думку та поведінку в умовах воєнного конфлікту» (Грищенко Д.О.).

19. Студент 202_СПД н. гр. ННІ № 3 НАВС **Забаштанський А.А.** «Особливості функціонування Ситуаційних центрів Національної поліції України в умовах воєнного стану» (к.ф.-м.н. Кудінов В.А.).

20. Студентка 102 БПМС н. гр. ННІ № 1 НАВС **Замула Д.В.** «Проблеми захисту даних у мережі Інтернет в умовах воєнного стану» (к.ю.н. Яровий К.В.).

21. Студентка 102 БПМС н. гр. ННІ № 1 НАВС **Іваненко К.В.** «Оптимізація роботи системи «ЦУНАМІ» в правоохоронних органах» (к.ю.н. Яровий К.В.).

22. Слухач магістратури НАВС **Ігонін О.Є.** «Безпека користування електронною поштою» (д.ф. Школьніков В.І.).

23. Курсант 204 н. гр. ННІ № 3 НАВС **Карпенко А.М.** «Роль сучасних технологій у забезпеченні безпеки інформації» (к.ю.н. Яровий К.В.).

24. Курсант 203 н. гр. ННІ № 3 НАВС **Кедик Є.М.** «Проблеми використання штучного інтелекту в комп'ютерних системах» (к.ю.н. Яровий К.В.).

25. Слухач магістратури НАВС **Ковальов Д.О.** «Фішинг як загроза в мережі Інтернет» (д.ф. Школьніков В.І.).

26. Курсант 204 н. гр. ННІ № 3 НАВС **Кошельник І.Л.** «Кіберзлочинність як загроза національної безпеки України» (к.ю.н. Яровий К.В.).

27. Курсант 201 н. гр. ННІ № 3 НАВС **Красненко В.К.** «Сучасні виклики кібербезпеки в Україні в умовах воєнного стану» (к.ю.н. Яровий К.В.).

28. Доцент кафедри прикладних інформаційних систем Київського національного університету ім. Тараса Шевченка, кандидат технічних наук, доцент **Краснощок В.А.**, директор інформаційного обчислювального центру головного центру інформаційних технологій Державного торговельно-економічного університету **Шестак Я.І.** «Захист інформації в прикладних інформаційних системах».

29. Професор кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, кандидат фізико-математичних наук, доцент **Кудінов В.А.** «Залежність криптостійкості паролю користувача інформаційних систем спеціального призначення від кількості можливих для використання символів».

30. Здобувач вищої освіти НАВС **Красько І.А.** «Загрози від кібератак в умовах воєнного стану» (Буренко О.В.).

31. Слухач магістратури НАВС **Малік Д.А.** «Фізична безпека» (д.ф. Школьніков В.І.).

32. Курсант 202 н. гр. ННІ № 3 НАВС **Лип'юк А.М.** «Використання можливостей соціальних мереж у ході розслідування та розкриття злочинів» (к.ю.н. Яровий К.В.).

33. Студентка 101_СМенеджмент н. гр. ННІ № 1 НАВС **Лукашенко Н.Д.** «Нормативно-правові основи функціонування єдиної інформаційної системи МВС України» (к.ф.-м.н. Кудінов В.А.).

34. Курсант 204 н. гр. ННІ № 3 НАВС **Матвійчук О.М.** «Сучасний стан кіберзлочинності в Україні в умовах воєнного стану» (к.ю.н. Яровий К.В.).

35. Курсант 203 н. гр. ННІ № 3 НАВС **Михайлюк І.О.** «Аналіз проблематики використання технології штучного інтелекту правоохоронними органами» (к.ю.н. Яровий К.В.).

36. Курсант 2 курсу факультету № 4 ХНУВС **Прозоров В.Т.** «Можливості використання технологій штучного інтелекту правоохоронними органами» (Рог В.Є.).

37. Курсант 201 н. гр. ННІ № 3 НАВС **Самойленко О.В.** «Аналіз механізмів протидії дезінформації у соціальних мережах» (к.ю.н. Яровий К.В.).

38. Курсант 204 н. гр. ННІ № 3 НАВС **Сидорук О.С.** «Деякі аспекти використання сучасного інформаційно-аналітичного забезпечення в Національній поліції України» (к.ю.н. Яровий К.В.).

39. Здобувач вищої освіти НАВС **Слободян О.С.** «Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану» (Буренко О.В.).

40. Курсант 212 н. гр. ННІ № 1 НАВС **Цимбал Є.А.** «Шляхи вирішення проблем кібербезпеки в Україні в умовах воєнного стану» (Буренко О.В.).

41. Курсант 1 курсу факультету № 1 ДонДУВС **Шило І.Є.** «Стратегії боротьби з дезінформацією у мережі Інтернет під час воєнного стану» (д.ф. Габорець О.А.).

42. Студентка 201_СПД н. гр. ННІ № 3 НАВС **Шляхова В.О.** «Правове забезпечення основних інформаційних підсистем інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (к.ф.-м.н. Кудінов В.А.).

43. Старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1, Голова ради молодих вчених НАВС, кандидат юридичних наук **Яровий К.В.** «Міжнародний досвід використання штучного інтелекту в умовах воєнного стану».

РЕЗЕРВНІ ДОПОВІДІ:

1. Слухач магістратури НАВС **Довгалюк Б.В.** «Безпека в мережі Інтернет» (д.ф. Школьніков В.І.).

2. Курсант 1 курсу факультету № 1 ДонДУВС **Шаєц І.Є.** «Social engineering as a method of shaping people’s consciousness» (д.ф. Габорець О.А.).

3. Курсант 210 навчальної групи ННІ № 1 НАВС **Козлинець В.О.** «Використання можливостей кримінального аналізу підрозділами Національної поліції України» (д.ф. Школьніков В.І.).

4. Слухач магістратури НАВС **Олексюк Р.А.** «Вішинг: сучасна загроза в мережі Інтернет» (д.ф. Школьніков В.І.).

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.

Деякі вчені лише дотепер звертали увагу на окремі аспекти кібербулінгу, тоді як інші аналізували лише проблематику булінгу та кібербезпеки. Роботи відомих дослідників, таких як С. Албул, Р. Грищук, М. Грінченко, С. Гнятюк, І. Діордіц, Л. Лушпай, Д. Лейн, О. Ожийова, В. Петросянець, С. Стельмах, А. Губко, Ю. Савальєв, О. Ліщинська, Н. Новікова, О. Корченко, В. Ліпкан, С. Мельник, В. Кащук, І. Катеренчук, В. Грохольський, П. Біленчук, І. Севкова та інших, включають аналізи цих тем, але дотепер не було проведено комплексного наукового дослідження.

Термін «кібербулінг» походить від двох англійських слів: «кібер» і «булінг». «Кібер» означає віртуальне комп`ютерне середовище; «Bull» означає бик, бугай, галаслива людина, в переносному значенні – дуже сильна агресивна людина.

Офіційний веб-сайт UNICEF надає таке визначення поняття кібербулінгу, а також приводить приклади цього явища:

- поширення брехні про когось або розміщення фотографій, які компрометують когось, у соціальних мережах;
- надсилання повідомлень або погроз, які ображають когось або можуть завдати комусь шкоди, через платформи обміну повідомленнями;
- видання себе за когось іншого/іншу і надсилання повідомлень іншим людям від його/її імені [1].

Як вказує В.М. Фурашев, кібербулінг – це новітня форма агресії, яка передбачає собою напади з метою завдання психологічної шкоди: насміхання, цькування, маніпулювання через інформаційно-комунікаційні засоби, а саме: мобільний телефон, електронну пошту, соціальні мережі й ін. [2, с. 73].

На нашу думку, кібербулінг або кібермоббінг, представляє собою сучасну форму агресії, яка включає в себе заподіяння страждань дітям один одному, а також жорстокі дії від дорослих, що здійснюються в Інтернеті за допомогою мобільних телефонів, комп'ютерів, електронної пошти, соціальних мереж тощо.

У сучасному віртуальному світі розповсюджені форми кібербулінгу, такі як анонімні загрози, надіслані телефонні дзвінки, тролінг, стеження, сексуальні домагання, флеймінг, розповсюдження обмов, шахрайство, кіберпереслідування та інші види насильства.

У цьому контексті слід відзначити, що механізм адміністративно-правового регулювання кібернетичної та інформаційної сфери спрямований на захист як національних інтересів, так і інтересів окремих осіб. Адміністративно-правові принципи виконують різноманітні функції, як загальні, так і спеціалізовані, щоб визначити основні заходи та засоби протидії різним негативним кіберзагрозам та кібератакам [3, с. 202].

Тобто встановлення адміністративно-правових засад кібербулінгу – це процес регулювання явища кібербулінгу та визначення заходів його протидії на цій основі. Аналіз існуючого законодавства України показує відсутність чіткого визначення кібербулінгу, що вимагає покращення.

Однак, оскільки кібербулінг є формою кіберзагроз, можна стверджувати, що адміністративні засади забезпечення кібернетичної та інформаційної безпеки в Україні в певній мірі охоплюють регулювання кібербулінгу, але потребують законодавчих коректівів.

Тому вважаємо, що для ефективного створення адміністративно-правової бази протидії кібербулінгу, важливо розуміти сутність поняття «адміністративно-правові засади». Зазначене включає в себе систему юридичних норм, що визначають суть, принципи, завдання, форми та види кібербулінгу.

У підсумку, ефективне розв'язання проблеми кібербулінгу потребує комплексного підходу, який базується на створенні та впровадженні відповідних адміністративно-правових засад. Ці засади мають включати чітке визначення термінів, принципів, завдань та форм кібербулінгу, а також ефективні механізми для його протидії. Важливо постійно оновлювати та вдосконалювати законодавство з питань кібербезпеки, а також проводити освітню та інформаційну роботу серед населення, зокрема серед молоді, щоб підвищити усвідомлення щодо наслідків кібербулінгу та методів його запобігання. Тільки взаємодія громадських організацій, урядових структур, освітніх закладів та інших зацікавлених сторін може призвести до зменшення випадків кібербулінгу та створення безпечного середовища в Інтернеті для всіх користувачів.

Список використаних джерел:

1. Кібербулінг: матеріал з офіційного сайту ЮНІСЕФ. URL: https://www.unicef.org/ukraine/cyberbulling (дата звернення: 09.04.2024).

2. Фурашев В. М. Інформаційна небезпека: Кібербулінг. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: матеріали міжнар. наук.-практ. конф. (м. Київ, 21 квіт. 2017 р.). Київ: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»; вид-во «Політехніка». 2017. Ч. II. С. 72–75.

3. Чумак В. В., Цебинога В. Ю. Правове регулювання протидії кібербулінгу в Україні. Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали міжнародної наук.-практ. конф. (м. Харків, 30.11.2018 р.) (МВС України, Харків. нац. ун-т внутр. справ; Консультат. місія Європейського Союзу). Харків, 2018. С. 202–204.

Биков Ігор Олегович
старший науковий співробітник науково-дослідної лабораторії з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ, Голова ради молодих вчених Одеського державного університету внутрішніх справ, кандидат юридичних наук, адвокат

АНТИКОРУПЦІЙНИЙ ВПЛИВ ВІДКРИТИХ ДАНИХ

Відкритість публічної інформації у поєднанні із простим доступом до неї не лише є показником прозорості публічного адміністрування, а і є інструментом у боротьбі з проявами корупції. Антикорупційний вплив відкритих джерел проявляється, серед іншого, у можливості громадянського суспільства отримувати безперешкодно доступ до такої інформації та аналізувати її, що має стати невід'ємною складовою сучасного антикорупційного стратегічного плану.

Використання відкритих даних у сфері антикорупційних заходів відкриває новий рівень взаємодії між владою та громадянським суспільством. Дана взаємодія може стати ключовим механізмом для забезпечення обліку та контролю над діяльністю органів державної виконавчої влади, що створює ефективну систему відкритості та відповідальності. Відкриті дані можуть бути інструментом виявлення корупційних схем, сприяють підвищенню прозорості управління та активізують громадський контроль за владою. Потенціал відкритих даних у боротьбі з корупцією використовується в комплексі антикорупційних заходів у ряді європейських країн.

Нормативно, національний законодавець, визначає поняття публічної інформації у формі відкритих даних, як публічну інформацію у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. Водночас очевидне оновлення та актуалізація такої інформації робить її актуальним джерелом даних, які є дозволеними для її подальшого вільного використання та поширення. Відповідно до норм національного законодавства, будь-яка особа може вільно копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов'язковим посиланням на джерело отримання такої інформації [1].

Використання відкритих даних сприяє ефективному контролю за діяльністю державних установ, удосконаленню надання державних послуг та розробці нових сервісів та інструментів.

На основі відкритих даних розроблено значну кількість продуктів, включаючи онлайн-сервіси, аналітичні модулі, застосунки та чат-боти, які користуються популярністю серед мільйонів користувачів щомісяця.

Оцінка впливу відкритих даних є надзвичайно важливою, оскільки вона дозволяє оцінити ефективність роботи органів влади та створює механізм для відстеження прогресу з часом. Крім того, відмітимо, що даний контроль може бути реалізований не лише зі сторони громадськості, а і зі сторони відповідних правоохоронних та антикорупційних органів, у тому числі і з використанням методологій OSINT при аналізі таких даних.

Крім того, практично значимим є проект Дія. Відкриті дані, який транслює рівень національного розвитку сфери відкритих даних [2]. Разом із тим, держава чітко встановлює які дані та у якій формі можуть бути розкриті, зазначене визначено постановою Кабінету Міністрів України № 835 від 21 жовтня 2015 року «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних» [3]. Проте, аналіз тексту показує, що даний документ врегулює виключно питання оприлюднення інформації для вільного та безкоштовного доступу, що стосуються державного сектору, не звертаючи уваги на приватний бізнес.

На основі відкритих даних правоохоронні органи можуть проводити аналіз та розробляти стратегії для протидії корупції, ідентифікації шляхів виявлення злочинів та виявлення підозрілих транзакцій. Використання цих даних також дозволяє вдосконалити роботу зі збору та аналізу інформації, що є важливим етапом у розслідуванні злочинів та прийнятті правозахисних рішень.

Завдяки відкритим даним правоохоронні органи можуть також підвищити свою взаємодію з громадськістю та іншими галузями влади, що сприяє покращенню відкритості та взаємодії в системі правоохоронного захисту. Такий підхід сприяє збільшенню довіри громадськості до правоохоронних органів та підвищенню їхньої ефективності в боротьбі з корупцією та злочинністю в цілому.

Ці дані відіграють важливу роль у забезпеченні прозорості, ефективності та відповідальності в діяльності державних органів, оприлюднення і доступ до інформації дозволяють не лише зменшити ризик корупції, а й забезпечує широкий громадський контроль та участь у вирішенні соціальних проблем.

Список використаних джерел:

1. Про доступ до публічної інформації. Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

2. Офіційний сайт Дія. Відкриті дані. URL: https://diia.data.gov.ua.

3. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних. Постанова Кабінету Міністрів України; Положення, Перелік, Порядок від 21.10.2015 № 835. URL: https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text

Бойчура Марія Юріївна
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

ПРОБЛЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Під час широкомасштабної агресії з боку російської федерації Україна стикається з різними формами кібератак. Агресор намагається перешкодити наданню електронних послуг, що призводить до порушення прав громадян та збоїв у роботі державних органів. Також маємо справу з фішинговими атаками через електронну пошту та порушенням цілісності та конфіденційності персональних даних, що створює інформаційно-психологічний тиск на населення.

У сучасних умовах, коли Україна перебуває в умовах воєнного стану, знання про цифрову грамотність, дотримання цифрового етикету та правила кібергігієни є важливими не лише для ІТ-фахівців, але й для будь-якого громадянина. З початком війни, фахівці з ІТ з усієї країни приєдналися до кіберполіції та успішно протистояли агресору. У результаті спільних заходів було зруйновано критично важливі інформаційні системи окупанта.

Зазначена робота ґрунтується на працях відомих українських науковців, таких як Бубело Б. [1], Погорецький М. [2], Шеломенцев В. [2], Савінова Н. [3], а також інших дослідників, які внесли значний вклад у вивчення проблеми кіберзлочинів та проведення попереднього розслідування з метою притягнення винних осіб до відповідальності за ці злочини. Незважаючи на це, зазначена тема залишається актуальною та потребує подальших досліджень. Тому деякі аспекти вимагають більш детального аналізу.

Насамперед, насьогодні зростає популярність створення кібервійськ, які мають на меті не лише захист критичної інформаційної інфраструктури від кібератак, але й проведення превентивних наступальних операцій у кіберпросторі. Зазначене включає в себе здійснення атак на критично важливі об’єкти противника шляхом викривлення інформаційних систем, які керують цими об’єктами.

Важливо виділити дві ключові особливості державного регулювання у сфері захисту кіберпростору.

По-перше, в Україні безпека кіберпростору має відповідати стандартам демократичної держави та принципам верховенства права, при цьому мінімізуючи потенційні обмеження прав людини на інформацію [4].

Тому, ми погоджуємось з думкою Гнатченка Д.Д., що кіберпростір виступає як ключовий канал для обміну інформацією в сучасному суспільстві та є важливою частиною його інформаційної сфери [5, с. 49].

По-друге, на рівні адміністративно-правового регулювання процесів кібербезпеки відсутні систематичні заходи державного регулювання у сфері захисту кіберпростору, і їх перелік не є чітко визначеним [6].

Наша думка полягає в тому, що сучасна практика національного нормотворення в цьому питанні залишає певні недоліки. Тому стратегія ефективного управління системою державного регулювання в сфері захисту кіберпростору повинна бути гнучкою і враховувати сучасні виклики та реалії. Вона має бути доповненою або уточненою відповідно до нових обставин.

Отже, наша думка, для вирішення проблем інформаційного забезпечення в Україні важливо дотримуватись основних правил кібергігієни щодо боротьби з фейками: віддавати перевагу лише офіційним та перевіреним джерелам інформації, уникаючи сумнівних постів у соціальних мережах [7, с. 45]. У той же час необхідно мати на увазі, що навіть довірені медіа та офіційні особи можуть допускати помилки, особливо у період воєнного стану.

Після того, як ви дізнаєтеся важливу новину, важливо зачекати на її підтвердження або спростування. У випадку з діпфейками ситуація стає складнішою, оскільки це підроблені відеозаписи, на яких може бути зображена публічна особа та почута її промова. Наприклад, у Центрі інформаційної безпеки повідомляли, що у мережі може з’явитися відеозвернення Президента Володимира Зеленського про капітуляцію, проте це технологія машинного навчання, спрямована на заплутування слухачів та розбиття бойового духу наших громадян. У таких випадках важливо звернути увагу на наступні ознаки: неприродний тон виступу, текстуру шкіри, тіні на обличчі, «мерехтіння кадру», кліпання очей і таке інше. Головне правило – довіряти лише офіційним джерелам інформації [8, с. 5].

Враховуючи вищевикладене, слід зазначити, що для вирішення нагальних проблем важливо додатково вивчати позитивний досвід країн НАТО у сфері захисту кіберпростору, проведення кібероперацій, навчання фахових спеціалістів та інше. Крім цього, досвід останніх десятиліть зі збройних конфліктів та широкомасштабна агресія росії проти України підтверджують, що у сучасній війні перемагає той, хто швидше адаптується до нових інформаційних технологій та впроваджує їх у життя, розвиває нові воєнні доктрини і концепції, що відповідають сучасним викликам.

Список використаних джерел:

1. Бурбело Б. А. Криміналістичні основи протидії кіберзлочинності. Актуальні питання розслідування кіберзлочинів: матеріали міжнародної науково-практичної конференції (Харків, 10 грудня 2013 р.). Харків: Харківський національний університет внутрішніх справ. 2013. С. 179–182.

2. Погорецький М., Шеломенцев В. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. № 8. С. 89–96.

3. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти: монографія. К. : ДКС, 2011. 342 с.

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

5. Гнатченко Д. Д. Державне регулювання у сфері захисту кіберпростору як компонент забезпечення інформаційної безпеки України. Київ. нац. торг.-екон. ун-т, 2020.

6. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

7. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). Сучасна спеціальна техніка. 2023. № 3 (74). С. 42-49.

8. Шестак Я. І. Кібергігієна у інформаційному просторі в умовах воєнного стану. Кібергігієна у інформаційному просторі в умовах воєнного стану. Тези V міжнародної науково-практичної конференції: «Інформаційна безпека та комп’ютерні технології». Центральноукраїнський національний технічний університет, Кропивницький, 2022. С. 5-6.

Борисова Катерина Євгенівна
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ, рядовий поліції

Науковий керівник:
Світличний Віталій Анатолійович
кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ

ПОТЕНЦІАЛ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ШІ) ДЛЯ ОПТИМІЗАЦІЇ НАДАННЯ ДОМЕДИЧНОЇ ДОПОМОГИ ПОЛІЦЕЙСЬКИМ

Відповідно до статті 12 Закону України «Про екстрену медичну допомогу» особами, які зобов'язані надавати домедичну допомогу людині у невідкладному стані, є поліцейські [1].

В контексті сучасних вимог до надання медичної допомоги, актуальності набуває питання оптимізації процесів надання домедичної допомоги поліцейським, адже з початком повномасштабного вторгнення росії на нашу територію, розгортанням агресії по відношенню до українців постало питання удосконалення системи захисту здоров'я населення. Інформаційні технології, зокрема штучний інтелект (далі – «ШІ»), що розглядаються як інструменти для підвищення ефективності та оперативності, на нашу думку, є факторами першочергової необхідності для надання допомоги. Тому ми переконані, що вчені та практики повинні зосередити увагу в цьому надважливому напрямку, та докласти зусилля до аналізу та популяризації питання використання.

Використання сучасних інформаційних засобів, таких як мобільні додатки та автоматизовані системи, може суттєво поліпшити якість та швидкість реагування поліцейських у наданні першої допомоги постраждалим, тим самим оптимізувати процес й забезпечити виконання покладеного на поліцейського завдання згідно з статтею 2 Закону України "Про Національну поліцію" [2].

Розглянемо різновиди інструментів та зазначимо переваги й недоліки при наданні домедичної допомоги поліцейським:

1. **Медичні ідентифікатори (додатки та розширення).** Технології, що дозволяють швидко отримувати доступ до медичної інформації (про стан здоров'я людини, її алергії, хронічні захворювання, групи крові тощо).

Переваги включають оперативність доступу до важливої інформації та можливість надання адекватної допомоги. Однак, недоліками можуть бути проблеми з конфіденційністю та безпекою даних [3].

2. **GPS-системи.** Для точного визначення місцезнаходження потерпілого та зв'язку з медичними установами, може суттєво поліпшити якість і швидкість надання першої допомоги.

Переваги включають швидкість реагування та точність локації. Проте, недоліками можуть бути недостатня точність у великих містах або в глибоких будівлях (інших важкодоступних місцях).

3. **Системи віддаленого моніторингу.** Впровадження систем віддаленого моніторингу стану постраждалих може допомогти у вчасному реагуванні на критичні стани та запобіганні їх ускладненням.

Переваги включають можливість надання допомоги в реальному часі та вчасну інтервенцію. Недоліками можуть бути обмежені можливості моніторингу у віддалених або важкодоступних місцях [4].

4. **Системи автоматичного виявлення тривог.** Ці системи можуть виявляти аварійні ситуації, такі як падіння або втрата свідомості, і автоматично викликати швидку допомогу.

Це допомагає забезпечити швидку реакцію на надзвичайні ситуації. Проте, недоліками можуть бути можливість помилкового спрацювання системи; можливість виникнення проблем з обслуговуванням та технічною підтримкою.

Кожен з цих інструментів має свої переваги і недоліки, тому важливо враховувати їх при виборі та використанні для оптимізації надання домедичної допомоги поліцейським.

На наше переконання, одним з наступних прогресивних кроків необхідно розглядати активне впровадження в Україні та популяризацію серед населення використання медичних ідентифікаторів та автоматизованих систем (ШІ). Дане питання не підіймалося раніше у працях вітчизняних наукових співробітників, проте, пов'язане з тематикою, дослідження вже проводилося в США (2023 р.). Дослідження наголосило на тому, що існує нагальна потреба в освіті покращити обізнаність щодо ідентифікаторів та подібних автоматизованих систем, щодо використання [5].

Отже, необхідність оптимізації процесів надання домедичної допомоги поліцейським стає більш актуальною у зв'язку з вимогами сучасної медичної практики, особливо у контексті складної ситуації, що виникла внаслідок агресії росії. Використання сучасних технологій, таких як мобільні додатки та автоматизовані системи, може значно покращити якість і швидкість реагування поліцейських у наданні першої допомоги постраждалим. Хоча кожен інструмент має свої переваги і недоліки, їх використання може оптимізувати процес надання допомоги поліцейським і допомогти виконати покладені на поліцейського завдання.

Для подальшого удосконалення системи надання домедичної допомоги поліцейським рекомендується активно впроваджувати та популяризувати серед населення використання медичних ідентифікаторів та автоматизованих систем (ШІ), що сприятиме підвищенню ефективності і оперативності надання допомоги.

Список використаних джерел:

1. Про екстрену медичну допомогу. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/5081-17#Text (дата звернення: 01.03.2024).
2. Про Національну поліцію. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/main/580-19#Text (дата звернення: 01.03.2024).
3. Як налаштувати Medical ID та опцію виклику SOS на iPhone та Apple Watch. iLand. URL: https://iland.ua/articles/http-iland-ua-articles-yak-nalashtuvaty-medical-id-ta-opcyu-vikliku-sos-na-iphone-ta-apple-watch/ (дата звернення: 05.03.2024).
4. Переваги віддаленого моніторингу пацієнтів для зменшення витрат і покращення здоров'я - DusunIoT. Dusun IoT: Embedded Hardware Vendor | IoT Gateway Sepcialist. URL: https://www.dusuniot.com/uk/blog/7-benefits-of-remote-patient-monitoring-reduce-costs-and-improve-health/ (дата звернення: 05.03.2024).
5. Medical information during trauma resuscitations: are smartphones the contemporary medical ID bracelet? - pubmed. PubMed. URL: https://pubmed.ncbi.nlm.nih.gov/37506430/ (date of access: 05.03.2024).

Васюта Юлія Володимирівна
ад'юнкт кафедри криміналістики та судової медицини Національної академії внутрішніх справ, капітан поліції

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИННОСТІ СПІЛЬНИМИ СЛІДЧИМИ ГРУПАМИ КРІЗЬ ПРИЗМУ КРИМІНАЛІСТИЧНИХ ІННОВАЦІЙ

В умовах сьогодення стрімкий розвиток інформаційних технологій супроводжується новими цілями, схемами та методами злочинної діяльності у кіберпросторі. Використання інформаційного середовища для вчинення кримінально протиправних діянь призводить до необхідності правоохоронним органам держав співпрацювати між собою та вдосконалювати свої знання, вміння та навички. Так, формування криміналістичних знань, застосування криміналістичних інновацій, а також новітніх технологій є своєрідною відповіддю на появу нових способів та механізмів злочинної діяльності в умовах дії воєнного стану під впливом тенденцій розвитку науки, техніки та суспільства.

Насамперед на розслідування кримінальних правопорушень у сфері кіберзлочинності впливає низка факторів.

По-перше, кіберзлочинність не має кордонів та швидко розповсюджується на міжнародній арені.

По-друге, майже кожен вид кримінального правопорушення може бути вчинено за допомогою інформаційних технологій та комп'ютерних мереж.

По-третє, динамічність вчинення кіберзлочинів супроводжується необхідністю взаємодії правоохоронних органів держав та міжнародних організацій під час розслідування цих кримінальних правопорушень, зокрема шляхом створення спільних слідчих груп.

Акцентуємо увагу на окремі статистичні дані щодо розслідування кримінальних правопорушень у сфері кіберзлочинності за участю міжнародних партнерів. Так, відповідно до звітної інформації щодо результатів роботи Департаменту кіберполіції Національної поліції України відомо, що у 2023 році кіберполіцейськими забезпечено проведення 18 міжнародних поліцейських операцій, за результатами яких задокументовано кримінальну протиправну діяльність злочинних угруповань. Наприклад, проведено багаторівневу міжнародну спецоперацію щодо учасників злочинного угруповання, які з 2018 року, використовуючи розроблені ними віруси-шифрувальники, здійснювали атаки на сервера провідних світових компаній. Для аналізу цифрових даних та припинення цієї злочинної діяльності було задіяно понад 20 правоохоронців з Франції, Німеччини, Норвегії, Федерального бюро розслідувань США. Також на території Нідерландів було створено спеціальну робочу групу та Віртуальний командний пункт задля невідкладного аналізу інформації, отриманої під час проведення слідчих процесуальних дій на території України. Крім того, скеровано до суду кримінальні провадження щодо протиправної діяльності 42 організованих груп і злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 191 учасник, якими вчинено 731 кримінальне правопорушення (547 тяжких та особливо тяжких), з яких: 438 – шахрайств, 20 – крадіжок, 12 – за ст. 255 КК України «Створення, керівництво злочинною спільнотою, а також участь у ній», 3 – привласнення, розтрата майна, 46 – у сфері господарської діяльності, 33 – у сфері використання електронно-обчислювальних машин, 14 – у сфері службової діяльності, 7 – у сфері обігу наркотичних засобів, 158 – інші [1].

Оскільки до складу спільної слідчої групи входять представники Національної поліції України, то потужним вектором для оцінки ключових загроз та ризиків організованої злочинності та тяжких злочинів є розробка фахівцями Департаменту інформаційно-аналітичної підтримки спеціалізованого програмного забезпечення – інформаційної підсистеми «SOCTA». Відповідний хід подій дозволяє оптимізувати процес узагальнення відповідей експертів щодо організованих груп та злочинних організацій, а також допомагає проаналізувати ризики та механізми боротьби з міжнародною злочинністю [2].

Окрім цього, спільна слідча група здійснює розслідування кримінальних правопорушень, зокрема кіберзлочинів, за аналітичної та криміналістичної підтримки Європолу.

Так, Європол надає допомогу у зборі та аналізі даних, що були здобуті законними методами з відкритих джерел, таких як медіа, теле- та радіомовлення, тобто проводить розвідку на основі відкритих джерел (OSINT) [3].

Також в цьому контексті слід зазначити, що невід'ємною частиною забезпечення розслідування міжнародних злочинів, зокрема вчинених у кіберпросторі, є бази даних. Прикладом однієї із подібних баз стала спеціально розроблена Євроюстом база даних для зберігання та аналізу доказової інформації – «Core International Crimes Evidence Database». У цій базі можна зберігати цифрові підтвердження та дані щодо вчинених кримінальних правопорушень, зокрема фотографії, відео- та аудіозаписи, супутникові та дронові знімки, показання свідків та потерпілих, результати медичних, криміналістичних та військових досліджень, інформацію про окремі матеріальні докази тощо. Євроюст гарантує безпечне зберігання цих матеріалів відповідно до стандартів захисту особистих даних. Додатково слід зазначити, що аналіз цих даних сприятиме покращенню координації національних та міжнародних розслідувань, усуненню проблем з паралельними розслідуваннями, стандартизації процесів пошуку та обробки конкретних доказів (відомостей), пов'язаних із певним кримінальним правопорушенням чи місцем події, а також виявленню недоліків у доказовій базі [4, с. 235-236].

Передусім розслідування кримінальних правопорушень у сфері комп'ютерних технологій стає викликом для спільних слідчих груп, з огляду на слідову картину кримінального правопорушення. Цифрові сліди вимагають новітніх підходів до їх збирання, зберігання, використання й дослідження у процесі доказування. Так, слід акцентувати увагу на цифрову криміналістику. Як стратегічний напрям у системі криміналістичної науки та правозастосовної практики розвиток цифрової криміналістики відбувається у різновекторній послідовності: від формування окремої наукової галузі в криміналістиці, з урахуванням міжнародних стандартів, до застосування спеціальних знань під час роботи із цифровими слідами та проведення судових експертиз. Оскільки розслідування кримінальних правопорушень у сфері комп'ютерних технологій насичене великим обсягом електронних доказів, то аналіз цієї доказової інформації є ресурсомістким завданням для членів спільної слідчої групи. Відтак, використання спеціальних знань під час проведення слідчих дій є невід'ємною частиною ефективного розслідування кіберзлочинів.

У свою чергу, слушною є думка О.М. Дуфенюк щодо специфіки розслідування порушення законів та звичаїв війни, з огляду на стрімкий розвиток цифрових технологій, що зумовлено: широкими можливостями користувачів смартфонів, інших засобів з функціями фото- та відеофіксації документувати

воєнні злочини, транслювати події онлайн, поширювати без кордонів інформацію через мережу Інтернет, засоби масової інформації тощо; можливостями моніторингу за різними об'єктами, встановлення їх геолокації, а також обробки даних за допомогою засобів кримінального аналізу та кіберрозвідки; цифровізацією криміналістичної та судово-експертної діяльності (застосування дронів, 3D сканерів, мобільних лабораторій ДНК, спеціалізованого програмного забезпечення та лабораторних інноваційних засобів), що підвищує якість, точність та швидкість збирання доказової інформації; поступовою трансформацією моделі кримінального провадження від паперової до електронної форми доказування [5, с. 52-53].

Таким чином, тенденції кіберзлочинності становлять загрозу суспільству не лише на державному, але й на міжнародному рівнях. Так, діяльність спільних слідчих груп є важливим механізмом подолання злочинних діянь у кіберпросторі. У свою чергу, члени особливої форми міжнародного співробітництва мають володіти фундаментальними знаннями у сфері цифрової криміналістики. Очевидно, що міжнародне співробітництво під час розслідування кримінальних правопорушень у сфері кіберзлочинності покликане розробити спільну стратегію боротьби з кіберзагрозами, посилити організаційно-тактичні зусилля під час проведення слідчих дій з розслідування кіберзлочинів та запобігти використанню кіберпростору у кримінально протиправних цілях.

Список використаних джерел:

1. Про результати роботи Департаменту кіберполіції Національної поліції України у 2023 році: звіт від 31 січ. 2024 р. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/.

2. A corrupting influence: the infiltration and undermining of europe's economy and society by organised crime. Luxembourg: Publications Office of the European Union. 2021. 105 p.

3. Europol established OSINT task force to support investigations of war crimes in Ukraine, 2023. URL: https://mvs.gov.ua/uk/news/jevropol-stvoriv-operativnu-robocu-grupu-osint-dlia-pidtrimki-rozsliduvan-vojennix-zlociniv-v-ukrayini.

4. Caianiello M. The role of the EU in the investigation of serious international crimes committed in Ukraine. Towards a new model of cooperation. European Journal of Crime, Criminal Law and Criminal Justice, 2022, 30. P. 219-237. DOI: 10.1163/15718174-30030002.

5. Dufeniuk O. Investigation of war crimes in Ukraine: challenges, standards, innovations. Baltic Journal of Legal and Social Sciences, 2022, 1. P. 46-56. DOI: https://doi.org/10.30525/2592-8813-2022-1-6.

Вишневська Марія Юріївна
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

СУЧАСНИЙ СТАН КІБЕРЗАХИСТУ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

Україна, з самого початку повномасштабної війни з російською федерацією, зіткнулася не лише з постійним обстрілом ракетами, але і з різноманітними видами кібератак у цифровому інформаційному просторі. Кібератаки, на які звертається увага, різняться за формою та метою: від спроб дестабілізації суспільно-політичної обстановки до атак на критичну інфраструктуру та незаконного доступу до конфіденційної інформації громадян.

Агресія російська у кіберпросторі принесла значні виклики для української кібербезпеки. Зокрема, надійний захист від кібератак став пріоритетним завданням для уряду та правоохоронних органів України.

Незважаючи на те, що проблеми кіберзахисту в Україні були предметом наукових дискусій у роботах Алпеєва А.С., Архіпова О.Є., Бакалинського О.О. Богданова О.М., Грибуніна В.Г., Горбатько О.В., Мохора В.В., Чепуренко Я.О. в даний час питання кіберзахисту в кіберпросторі є найбільш розповсюдженим і актуальним для суспільства, оскільки це стосується всіх, хто має справу з інформаційними технологіями.

У цьому контексті, аналіз сучасного стану кіберзагроз та заходів захисту в Україні є надзвичайно важливим для розуміння проблеми та розробки ефективних стратегій протидії. Дослідження цих питань має на меті не лише виявлення потенційних ризиків та вразливостей, але й розробку практичних рекомендацій та інноваційних підходів до підвищення кібербезпеки в Україні.

На рівні адміністративно-правового регулювання процесів кібербезпеки відсутні систематичні заходи державного регулювання у сфері захисту кіберпростору і їх перелік не є чітко визначеним [1].

Крім цього, сьогодні, коли наша держава знаходиться в умовах воєнного стану важливим є не лише для ІТ-фахівців, але й для будь-якого громадянина навчання застосування цифрової грамотності, дотримання цифрового етикету та правил кібергігієни.

З початком війни ІТ-фахівці з усієї країни долучилися до кіберполіції та зуміли дати відсіч агресору. В результаті злагоджених дій були виведені з ладу критично важливі інформаційні системи окупанта.

Найбільшу активність від атак російських хакерів відчувають на собі державні та місцеві органи влади, інформаційні ресурси сектору безпеки та оборони, енергетичний, фінансовий і комерційний сектори, а також ІТ-інфраструктура та транспортна галузь. Наразі хакери все більш активно атакують енергетичний сектор, щоб позбавити українців умов для нормального життя навіть поза окупованими територіями, де вони фізично знищують інфраструктуру населених пунктів.

Щодо мети кібератак, то в 306 випадках здійснювався несанкціонований збір інформації, у 267 – були спроби розмістити шкідливий програмний код, у 149 – спроби втручання у функціонування роботи ресурсів, інші різновиди атак – 401 [2].

Слід зазначити, що війна відбувається не лише на фізичному фронті, а й у інформаційному полі. Загарбники здійснюють кібератаки не лише на урядові структури – жертвами зламів і викрадення даних стають і пересічні громадяни. Вони намагаються отримати доступ до персональних даних та державних реєстрів через приватні комп'ютери та мобільні телефони. Українці масово отримують листи із шкідливою програмою, яка викрадає паролі й файли.

Проте українцям необхідно дотримуватися вимог кібергігієни, оскільки інформаційний простір це джерело поширення фейків, діпфейків, підробки сайтів, фішингових атак, заволодіння акаунтами громадян [3, с. 46].

Розглянемо детальніше основні правила кіберзахисту в Україні, які виникають в умовах воєнного стану. Передусім, важливо дотримуватись основного принципу кібергігієни щодо фейків: слід читати лише із офіційних та перевірених джерел. Однак у воєнний час слід мати на увазі, що навіть надійні медіа та офіційні особи можуть допускати помилки. У таких обставинах українці постійно оновлюють стрічку новин, щоб дізнатися про ситуацію на фронті та в дипломатичному полі. Тим часом ворог активно розповсюджує фейки про виглядання міст, капітуляцію України чи евакуацію місцевих мешканців.

Крім цього, якщо мова йде про сторінки в соціальних мережах, важливо звернути увагу на те, чи має аккаунт верифікацію (синя галочка поруч із назвою). Ще однією ознакою є невелика кількість підписників та дописів. Щодо веб-сайтів, варто звернути увагу на наявність символу замочка в адресному рядку браузера, що свідчить про успішну перевірку та отримання сертифіката безпеки. Додатково можна скористатися сервісом Whois для перевірки дати реєстрації/створення сайту, власності компанії та інших юридичних даних. Ще один вдосконалений метод фішингу – підробка посилань на підпис електронних петицій.

DeepFakes (контамінація Deep Learning та Fake, англ. – фальшивка) є продуктом двох алгоритмів ШІ, які взаємодіють у так званій Generative Adversarial Network (укр. генеративній змагальній мережі) [3, с. 17].

Іншими словами, діпфейк – це підроблене відео, на якому можна побачити публічну особу з виступом, а також чути її голос. Наприклад, у Центрі інформаційної безпеки повідомляли, що в мережі може з'явитися відеозвернення Президента Володимира Зеленського, в якому він, мабуть, оголосить про капітуляцію. Проте це використання технології машинного навчання, яка може бути застосована для збентеження та підірвання бойового духу.

Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі.

Отже, встановлено, що нова ера кібербезпеки вимагає цілком нових підходів до управління ресурсами, зокрема інформаційними. Успіх таких змін значною мірою залежить від того, як гнучко організовані процеси на рівні держави, а також як імплементуються нові моделі та методи роботи у боротьбі з можливими загрозами.

Наша точка зору полягає в тому, що для вирішення проблем інформаційного забезпечення в Україні важливо дотримуватись основних правил кібергігієни у боротьбі з фейками, діпфейками, підробкою сайтів, фішинговими атаками, заволодінням акаунтами громадян: надавати перевагу лише офіційним та перевіреним джерелам інформації, уникаючи підозрілих постів у соціальних мережах. Одночасно слід мати на увазі, що навіть довірені медіа та офіційні особи можуть допускати помилки, особливо у період воєнного стану.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. Як забезпечити захист кіберпростору України на тлі збройної агресії рф. Інформаційний Інтернет-ресурс URL: https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf.

3. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). Сучасна спеціальна техніка. 2023. № 3 (74). С. 42-49.

4. Вальорска М. Аґнєшка. Діпфейк та дезінформація: практ. посіб. / Аґнєшка М. Вальорска ; пер. з нім. В. Олійника. Київ : Академія української преси; Центр Вільної Преси, 2020. 36 с.

Войцеховська Дар'я Миколаївна
курсант 204 навчальної групи ННІ № 3 НАВС, капрал поліції

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

СТАН ДОСЛІДЖЕННЯ ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Зростання злочинності та вдосконалення методів їх вчинення ускладнюють роботу правоохоронних органів. У відповідь на це Національна поліція України (далі – НПУ) активно впроваджує нові інформаційні технології та системи, які допомагають їй ефективніше розкривати злочини, забезпечувати громадський порядок та безпеку громадян.

Проблематика інформаційного забезпечення правоохоронних органів вивчалися різними фахівцями з різних наукових галузей. Зазначене свідчить про комплексний підхід до розвитку наукової думки в цьому напрямку. Наприклад, І.Р. Бондар [1] розробив алгоритм управління програмою безперервності функціонування системи інформаційної безпеки держави. О. Панченко [2] дослідив питання державного управління у сфері забезпечення інформаційної безпеки в контексті різних дестабілізуючих факторів. Б.В. Паш [3] розглянув сутність та структуру інформаційної безпеки в умовах глобалізації. Є.В. Кобко дослідив місце інформаційної безпеки в структурі національної безпеки через аналіз сучасного стану та перспектив правового регулювання відповідних суспільних відносин [4]. М.Т. Гаврильців зосередився на дослідженні сутності інформаційного захисту як складової національної безпеки України в умовах гібридної війни [5].

На нашу думку, для вирішення проблеми інформаційного забезпечення правоохоронних органів необхідно посилити розвиток програмного забезпечення та співпрацю з науково-дослідними установами, щоб забезпечити постійне оновлення та підвищення кваліфікації персоналу у сфері кібербезпеки.

Підрозділи інформаційно-аналітичної підтримки в Національній поліції керують використанням сучасних інформаційних технологій, забезпечуючи функціонування ІПНП в рамках ЄІС МВС та оперуючи інформаційними ресурсами. Серед їхніх завдань – створення та супровід автоматизованих систем,

забезпечення доступу до інформації, створення підсистем ЄІС МВС та формування баз даних різного характеру.

Основні завдання цих підрозділів включають:

- забезпечення роботи комплексної інтегрованої системи, яка підтримує функціонування суб'єктів системи, надає їм інформаційну підтримку та обслуговує їх діяльність. Зазначене включає розробку та підтримку програмного забезпечення, технічні засоби зв'язку, обробку та захист інформації;
- створення та підтримка інформаційних ресурсів, які представляють собою групи взаємозв'язаних даних, об'єднаних в системах МВС за певними критеріями, включаючи пріоритетні інформаційні ресурси;
- забезпечення доступу до інформаційних ресурсів інших органів державної влади, включаючи пріоритетні ресурси МВС;
- розробка та підтримка підсистем Єдиного інформаційного простору МВС, зокрема Інформаційного порталу Національної поліції України та його компонентів;
- виконання інших завдань інформаційного, інформаційно-аналітичного, технічного та технологічного характеру [6, с. 278].

Враховуючи вищевикладене слід зазначити, що для удосконалення роботи підрозділів НПУ, які відповідають за використання сучасних інформаційних технологій та реалізацію функцій ІПНП в рамках ЄІС МВС, можна розглянути наступні шляхи удосконалення:

1) оптимізація інтегрованої системи (вдосконалення програмного забезпечення та технічні засоби зв'язку, щоб забезпечити ефективне функціонування системи);

2) розвиток інформаційних ресурсів (розширення та покращення існуючих інформаційні ресурси, забезпечуючи їх відповідність потребам і вимогам поліцейської діяльності);

3) підвищення доступності інформаційних ресурсів (забезпечення зручного та безпечного доступу до інформації для інших органів державної влади та внутрішніх користувачів, зокрема через розробку спеціалізованих інтерфейсів та засобів авторизації);

4) оновлення та підтримка підсистем (забезпечення постійної підтримки та оновлення існуючих підсистем ЄІС МВС, включаючи ІПНП, з метою забезпечення їхньої ефективної роботи та відповідності сучасним вимогам);

5) регулярне навчання та підвищення кваліфікації персоналу (забезпечення ефективного використання інформаційних технологій, персонал повинен постійно підвищувати свою кваліфікацію та навчатися використовувати нові інструменти та методи аналізу даних).

На нашу думку зазначені шляхи вдосконалення інформаційного забезпечення НПУ можуть сприяти покращенню роботи та підвищенню їхньої ефективності під час розслідування та розкриття злочинів правоохоронними органами.

Список використаних джерел:

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.
2. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. 2019. Випуск 3. URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf (дата звернення: 15.04.2024).
3. Паш Б. В. Складові інформаційної безпеки держави: постановка питання. Закарпатські правові читання. 2017. Том 1. С. 509–512.
4. Кобко Є. В. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. National law journal: teory and practice. 2019. March. С. 46–50.
5. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203.
6. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 23 грудня 2016 року / упорядник Т. В. Магеровська /. Львів : ЛьвДУВС, 2017. 313 с.

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs

OSINT: A SCIENTIFIC APPROACH TO INFORMED DECISION-MAKING

In the current era of rapid technological progress and widespread internet availability, Open Source Intelligence (OSINT) technologies hold significant sway over the sourcing, analysis, and utilization of information. This dominance stems from their capacity to systematically navigate the vast expanse of digital data, extracting valuable insights crucial for informed decision-making across various domains.

OSINT entails the systematic gathering, examination, and utilization of publicly available information from diverse sources to draw meaningful conclusions and comprehend various situations. This methodology finds application across intelligence, cybersecurity, competitive analysis, law enforcement, and other sectors where access to open information enhances decision-making processes. It relies on sources like social media, public databases, websites, and forums.

Within the domain of OSINT, researchers and analysts harness specialized tools and techniques to collect, assess, and interpret vast amounts of data, thereby extracting

valuable insights [1, p. 92]. This process encompasses revealing information about individuals, companies, organizations, events, technologies, and other pertinent subjects.

However, due to the multifaceted nature of OSINT and the array of associated tools, our focus narrows to a specific aspect within this expansive field - the OSINT Framework. This framework comprises tools and resources tailored to gather and analyze information from publicly available internet sources, facilitating exploration, monitoring, and analysis of various data types to identify patterns, trends, and potential threats. Leveraging OSINT proves indispensable across diverse domains such as cybersecurity, fraud prevention, criminal investigations, incident analysis, and intelligence operations. The abundance of openly accessible internet data provides valuable insights into pinpointing threats, vulnerabilities, suspicious activities, and emerging trends, benefiting both commercial and public sectors by supporting decision-making, compiling statistics, monitoring social media, and gauging public sentiment.

Effectively employing OSINT requires adept skills in information searching, filtering, and analysis, alongside adherence to legal and ethical considerations regarding open information access. This article serves as a valuable resource compilation for newcomers to the OSINT and infosec fields, while seasoned professionals will find it enriching with useful information and unique materials.

Open Source Intelligence involves utilizing publicly available sources to acquire and assess information accessible to the general public, with the primary aim of comprehending given situations or entities through processing and analyzing openly accessible data. With technological advancements and data proliferation, OSINT offers extensive application opportunities across various domains.

In the realm of social networks and media, OSINT encompasses activities such as monitoring social media platforms for interactions, community dynamics, and key individuals, as well as tracking news and content from diverse sources to grasp the prevailing situation.

In geospatial analysis, OSINT utilizes geodata including satellite imagery and geographic information systems to locate objects and scrutinize spatial relationships, while textual and visual information analysis involves employing natural language processing (NLP) algorithms and computer vision technologies.

Integral to OSINT are data analysis platforms like Maltego and Recorded Future, along with ethnographic analysis focusing on sociocultural learning to understand behavioral patterns and cultural differences for effective information contextualization.

These OSINT tools find applications across security, intelligence, business intelligence, and more, incorporating scientific methodologies and technologies to optimize data collection and analysis, thereby facilitating well-informed decision-making processes.

References:

1. Zhmur N.V. Mezhdunarodno-pravovye standarty zashhity informacii: otdelnye aspekty. Legeasi Viata. 2014. № 2/2 (266). S. 90-93.

Глущенко Іван Олександрович
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ, рядовий поліції

Науковий керівник:
Світличний Віталій Анатолійович *кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ*

ДЕЯКІ ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ ПОЛІЦІЇ УКРАЇНИ

Вступ. Штучний інтелект, впроваджений в різноманітні сфери життя в умовах цифрової революції, дозволяє вирішувати складні завдання за допомогою наукових методів досліджень та обробки інформації. Ця технологія дозволяє створювати та використовувати бази знань, моделі ухвалення рішень і алгоритми роботи з інформацією, щоб досягти поставлених цілей.

Виклад основного матеріалу. Принципи та завдання розвитку технологій штучного інтелекту в Україні законодавчо визнано одним із пріоритетних напрямів у сфері науково-технологічних досліджень. Україна, яка є членом Спеціального комітету із штучного інтелекту при Раді Європи, у жовтні 2019 року приєдналася до Рекомендацій Організації економічного співробітництва і розвитку з питань штучного інтелекту (Organization for Economic Cooperation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449) [1].

Використання можливостей ШІ у роботі правоохоронних органів, зокрема у напрямі протидії злочинності, є практично затребуваним та актуальним. Можливості програмного забезпечення в частині підтримання правопорядку дають значну перевагу людському потенціалу щодо фіксації, попередження та завчасного реагування на правопорушення. Однією з головних можливостей є використання аналітики даних і машинного навчання для прогнозування злочинів, виявлення злочинців та аналізу моделей злочинності. Це дозволяє правоохоронним органам зосередити свої ресурси на тих областях, де ймовірність виникнення злочину найвища, сприяючи попередженню злочинів та збільшенню рівня безпеки.

Уже сьогодні вітчизняні правоохоронні органи активно використовують технології ШІ за такими основними напрямками.

1. *Виявлення злочинців та злочинних груп*: ШІ може аналізувати великі обсяги даних, включаючи відео- та аудіозаписи, соціальні медіа, телефонні розмови тощо, для виявлення злочинців та злочинних груп [2].

2. *Прогнозування злочинів*: ШІ може аналізувати статистичні дані та інші джерела інформації для прогнозування місць та часу можливих злочинів. Це дозволяє правоохоронним органам приймати превентивні заходи та зосереджувати свої ресурси на потенційно небезпечних місцях [2].

3. *Аналіз доказів*: ШІ може допомогти правоохоронним органам аналізувати великі обсяги доказів, такі як відеозаписи, фотографії, документи тощо, для виявлення важливих деталей та зв'язків, які можуть бути корисними під час розслідування [2].

4. *Автоматизована обробка заяв та документів*: ШІ може автоматизувати процес обробки заяв та документів, що надходять до правоохоронних органів. Це дозволяє збільшити швидкість та точність обробки інформації, а також зменшити навантаження на працівників [3].

5. *Використання систем відеоспостереження*: ШІ може аналізувати відеозаписи з систем відеоспостереження для виявлення підозрілих дій, розпізнавання об'єктів та ідентифікації осіб [3].

6. *Перевірка документів та ідентифікація осіб*: ШІ може автоматично перевіряти документи, такі як паспорти та водійські посвідчення, для виявлення підробок. Він також може допомогти в ідентифікації осіб на основі фотографій.

Таким чином, технології штучного інтелекту відкривають нові можливості для правоохоронних органів у виконанні своїх обов'язків. Ці технології допомагають забезпечити поліпшення ефективності і точності роботи правоохоронних органів у багатьох аспектах. Однією з головних можливостей є використання аналітики даних і машинного навчання для прогнозування злочинів, виявлення злочинців та аналізу моделей злочинності. Це дозволяє правоохоронним органам зосередити свої ресурси на тих областях, де ймовірність виникнення злочину найвища, сприяючи попередженню злочинів та збільшенню рівня безпеки. Технології штучного інтелекту також можуть використовуватись для автоматизованого аналізу великого обсягу даних, включаючи відеозаписи, зображення, текстові повідомлення тощо.

Однак, варто враховувати етичні та конституційні аспекти використання таких технологій. Необхідно забезпечити конфіденційність та безпеку зібраних даних, а також уникати можливих форм дискримінації або зловживання владою. Отже, правоохоронним органам необхідно розробляти і впроваджувати політики та стратегії, які забезпечать відповідальне та етичне використання технологій штучного інтелекту.

Висновки. Узагалі, використання технологій штучного інтелекту може значно покращити роботу правоохоронних органів, сприяючи збільшенню ефективності, точності та безпеки. Проте, необхідно забезпечити баланс між використанням цих технологій та захистом основних прав та свобод людей.

Ефективність використання штучного інтелекту залежить від способу й персоналу, що його використовує, а також від цілей, на які він спрямований. IT-технології, у тому числі штучний інтелект, можуть стати криміногенним чинником в майбутньому, сприяти злочинності або навіть породжувати нові види злочинності. Це визначає напрями для подальших наукових досліджень.

Список використаних джерел:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р // Кабінет Міністрів України: офіц. сайт. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 (дата звернення: 16.04.2024)

2. Lviv State University of Internal Affairs Institutional Repository (LvSUIAIR): Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. Lviv State University of Internal Affairs Institutional Repository (LvSUIAIR): Головна сторінка. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/5945 (дата звернення: 16.04.2024).

3. Можливості використання штучного інтелекту у кримінальному провадженні в Україні.| Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Право». Наукова періодика Каразінського університету. URL: https://periodicals.karazin.ua/law/article/view/22344 (дата звернення: 16.04.2024).

Головко Олександр Віталійович
курсант 208 навчальної групи ННІ № 1 НАВС, рядовий поліції

Ботнаренко Ірина Анатоліївна
кандидат юридичних наук, старший науковий співробітник наукової лабораторії з проблем протидії злочинності ННІ № 1 НАВС

АСПЕКТИ ТА ПИТАННЯ КІБЕРБЕЗПЕКИ ДЛЯ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

У сучасному світі інформаційних технологій та становлення інформаційного суспільства виникають нові виклики та загрози у сфері кібербезпеки. Обсяг персональних даних, які збираються підприємствами, організаціями, державними установами та урядами, швидко зростає. Ці особисті дані використовуються для створення профілів людей, прогнозування та контролю їхньої поведінки.

З одного боку, це може забезпечити персоналізований досвід та ефективніше використання ресурсів, проте з іншого боку, це створює ризики дезінформації та зловживання зібраними даними.

Проблема конфіденційності даних. Основною проблемою конфіденційності, з якою стикаються розробники та користувачі інформаційних систем, є захист конфіденційності персональних даних. Багато організацій досі зберігають приватну інформацію та навіть паролі в незашифрованому вигляді. Незважаючи на прогрес у протоколах безпеки, кількість порушень конфіденційності продовжує зростати. Згідно зі звітом Risk Based Security, загальна кількість скомпрометованих записів у 2022 році перевищила 37 млрд [1].

Порушення даних відбувається через несанкціонований доступ до баз даних організацій, що дозволяє хакерам викрасти конфіденційну персональну інформацію, включно з паролями, номерами кредитних карток, номерами соціального страхування та банківськими даними. Ці добре задокументовані інциденти мали негативні наслідки, такі як шахрайство з кредитними картками та крадіжка особистих даних [2].

Ситуація в Україні. В Україні в умовах війни з росією інтенсивність кібератак з боку російських хакерів не зменшується. Найбільше атакам піддаються уряд, місцеві органи влади, оборонний, фінансовий та енергетичний сектори, транспортна інфраструктура та телекомунікаційна галузь. Спостерігається неухильне зростання кіберзлочинності, метою якої є крадіжка або знищення інформації, дестабілізація ситуації в країні, виведення з ладу державних установ та обладнання.

Для протидії зростанню кіберзлочинності був прийнятий Закон «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам» № 2137-IX [3], який спрощує процедуру розслідування кіберзлочинів, та Закон «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX [4], які вносять зміни до Кримінального кодексу з метою посилення відповідальності за кіберзлочини. Проте для підвищення рівня кібербезпеки необхідно забезпечити належний захист державних установ та об’єктів критичної інфраструктури, а також підвищувати обізнаність громадян про кіберзагрози [5].

Наразі у нас в країні надзвичайно слабке становище в питанні, що стосується інформаційної війни з росією. Країна-агресорка є державою, яка веде інформаційну війну одна з найкращих у світі. Про це свідчить масова пропаганда, яка створюється не лише для росіян, що спрямована на їх «зомбування», а також і безпосередньо на громадян України. Вся ця робота росії спрямована на погіршення морального духу українців, адже велика кількість ІПСО демотивує українців на боротьбу з росією і це на користь країні-агресору.

В якості прикладу можна зазначити інтернет-ботів, які представляють із себе звичайних людей, проте насправді це просто фейк. Одна з їхніх робіт полягає в сіяні розладу між українцями. Так вони намагаються зробити внутрішні міжусобиці, які негативно впливають на український дух серед громадян. Це лише один приклад дії інформаційної війни росії. До того ж дезінформація зі сторони росії спрямована не тільки на прямі сторони конфлікту, а ще й союзників нашої держави. Надзвичайно велика пропаганда спрямована на європейців та на американців, які є прямими нашими союзниками та від їхньої допомоги залежить наше становище в цій довготривалій війні. У 2024 році вийшло інтерв’ю Такера Карлсона з володимиром путіним. Воно було спрямоване на виправдання російської агресії проти України та мало на меті перетягнути якнайбільше іноземців на бік підтримки росії. Є достатня кількість іноземців, які стали жертвами цієї дезінформації, тому Україні треба якнайкраще боротися в інформаційній війні та впроваджувати свої нові методи боротьби з ними або запозичувати їх у країн Європи, які можуть допомогти з цим.

Законодавче регулювання. У відповідь на зростання кіберзлочинності та занепокоєння користувачів з приводу конфіденційності їхніх даних пропонується та впроваджується законодавство щодо захисту персональних даних. Проте наразі існують недоліки у законодавчому регулюванні кібербезпеки в Україні. Зокрема, відсутній уніфікований понятійно-термінологічний апарат, є невідповідність визначень чинним актам та міжнародним документам, окремі норми застаріли, повільно впроваджується європейське законодавство. Нормативно-правові акти розрізнені, бракує кодифікованого акту.

Пропонується формування Інформаційного кодексу України як зводу інформаційно-правових норм, зокрема з питань кібербезпеки. Необхідно узгодити понятійно-термінологічний апарат відповідно до національних та міжнародних актів, посилити відповідальність за кіберправопорушення та імплементувати положення європейського законодавства.

Євроінтеграція у сфері кібербезпеки. Для ефективної євроінтеграції України потрібна реалізація державної політики у сфері кібербезпеки відповідно до європейських норм і стандартів. Органи виконавчої влади мають стати провідними суб'єктами впровадження євроінтеграційного курсу в цій сфері. Необхідна співпраця з ЄС та НАТО, залучення кращих світових практик і експертизи. Слід підвищувати кіберстійкість України відповідно до стандартів ЄС, реформувати органи кібербезпеки згідно з євроінтеграційними вимогами.

Кібербезпека займає особливе місце в сучасних наукових дослідженнях і активно розвивається з кожним роком. Сама концепція кібербезпеки вимагає переосмислення через швидкі зміни у сфері інформації та зростаючу "інформаційну" складову розвитку світової спільноти [6].

Підсумовуючи, можна зазначити, що забезпечення кібербезпеки є одним з найважливіших завдань у сучасному інформаційному світі.

Необхідно вдосконалювати законодавчу базу, впроваджувати передові практики та технології захисту інформації, а також підвищувати обізнаність громадян про кіберзагрози. Лише комплексний підхід, що поєднує правове регулювання, технічні рішення та освіту громадськості, дозволить ефективно протидіяти зростаючим кіберзагрозам та захистити конфіденційність персональних даних. Для України, що прагне євроінтеграції, питання кібербезпеки набуває особливого значення в умовах війни з росією та необхідності посилення обороноздатності держави.

Список використаних джерел:

1. RiskBased Security. 2022 Year End Report: Data Breach Quickview. URL: https://flashpoint.io/resources/report/state-of-data-breach-intelligence-2022-midyear.

2. Балацька Валерія Сергіївна, Опірський Іван Романович. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. URL: https://journals.indexcopernicus.com/search/article?articleId=3786215.

3. Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам : Закон України від 15.03.2022. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text

4. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.

5. Смілянець Єгор Ігорович, Білаш Олексій Олександрович, Плахотний Артем Павлович. Щодо кібербезпеки в умовах воєнного стану. URL: https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/936.

6. Зуй В. В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_1/35.pdf.

Гордієнко Данило Сергійович
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ, рядовий поліції

Науковий керівник:
Світличний Віталій Анатолійович *кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ*

ОСНОВНІ ТЕХНІКИ ЗБОРУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ В УМОВАХ ВОЄННОГО СТАНУ

Вступ. Використання розвідувальних даних з відкритих джерел (OSINT) може стати ключовим інструментом у різних сферах у майбутньому.

Виклад основного матеріалу. У сфері безпеки і боротьби з тероризмом OSINT може допомагати відстежувати діяльність терористичних груп та розкривати їхні плани, аналізуючи загальнодоступну інформацію. У кризовому управлінні ці дані також можуть бути використані для оперативної реакції на загрози та кризи. В політичному аналізі OSINT може надати важливу підтримку, збираючи та аналізуючи дані з різних відкритих джерел і розуміючи громадську думку та настрої. У сфері економічного аналізу OSINT може відстежувати ринкові тенденції та допомагати у розумінні потоків капіталу та прийнятті обґрунтованих економічних рішень. Автоматизований аналіз великих обсягів медіа-контенту за допомогою OSINT може покращити аналітичні можливості в аналізі ЗМІ. У наукових дослідженнях OSINT може стати ключовим інструментом для збору та аналізу даних, що дозволить отримувати більш точні результати. У сфері кібербезпеки OSINT може допомагати виявляти потенційні загрози та вразливості в мережах.

Загалом, використання OSINT може стати дуже важливим і корисним у різних галузях, оскільки він надає доступ до великих обсягів відкритої інформації [1]. Нижче подано приклади систем OSINT:

- моніторинг соціальних мереж дозволяє в реальному часі спостерігати за суспільними настроями та пересуванням військ;
- аналіз загальнодоступних джерел новин і звітів надає інформацію про події на полі бою та зміни військових позицій;
- використання супутникових знімків дозволяє в реальному часі відстежувати переміщення військ та інфраструктури;
- аналіз географічних даних допомагає ідентифікувати споруди та місцевість [2] та виявляти потенційно вразливі райони.

Розвиток і вдосконалення методів збору та аналізу даних стає невід'ємною складовою в сучасному суспільстві, де доступ до великих обсягів інформації стає все більш швидким. Швидкий прогрес технологій вимагає постійного удосконалення методів, щоб забезпечити ефективність та точність результатів. Збільшення інвестицій у дослідження та розробку нових інструментів є критично важливим для прогресу в цій сфері. Інвестиції в нові технології, програмне та апаратне забезпечення дозволять створити потужні інструменти для збору, обробки та аналізу даних. Зміцнення співпраці між державними установами є ключовим чинником ефективного використання отриманої інформації, що сприяє обміну ресурсами та покращує аналітичні можливості. Навички та підготовка фахівців у сфері розвідки мають велике значення для успішного використання інформації, і належна освіта може гарантувати, що фахівці володіють необхідними знаннями та навичками. Встановлення суворих стандартів етичного використання інформації є ключовим для забезпечення конфіденційності та захисту приватності, а оновлення методів збору та аналізу даних дозволяє збирати та обробляти інформацію більш ефективно. Розробка міжнародних стандартів для обміну інформацією важлива для підтримки співпраці між різними країнами та організаціями, сприяючи ефективній аналітичній роботі за загальноприйнятими правилами та процедурами.

Висновки. В умовах воєнного стану виникають дуже напружені обставини, коли зібрання та аналіз інформації стають критично важливими для успішності операцій і збереження людських життів. У таких обставинах інструменти OSINT стають неодмінною складовою стратегії військового керівництва та управління. Основні методи збору інформації, такі як моніторинг соціальних мереж, дозволяють в реальному часі спостерігати за подіями в зонах конфлікту та виявляти зміни в громадській думці і настроях. Аналіз новин і повідомлень з відкритих джерел може надати більш детальну інформацію про різні аспекти конфлікту, такі як стратегічні позиції і рух військ. Супутникові знімки та аналіз географічних даних можуть забезпечити об'єктивні дані про територію, інфраструктуру та рухи військ противника.

Проте в усіх цих випадках надзвичайно важливо дотримуватися етичних стандартів та захищати особисті дані. Забезпечення конфіденційності та приватності даних важливо не лише з етичних міркувань, але й для запобігання можливим репресіям і діям, які порушують права людини. Загалом, використання інструментів OSINT в умовах воєнного конфлікту може виявитися вирішальним чинником для прийняття правильних військових стратегічних та тактичних рішень. Швидке отримання, аналіз та використання критично важливої інформації може забезпечити ефективну відповідь на виклики воєнного конфлікту.

Список використаних джерел:

1. Розвідка на основі відкритих джерел. Інформаційний Інтернет-ресурс Вікіпедія. URL: https://uk.wikipedia.org/wiki/Розвідка_на_основі_відкритих_джерел (дата звернення: 17.04.2024).

2. Що таке OSINT і як він допоміг викрити вбивства у Бучі. Explainer - пояснюємо новини. Інформаційний Інтернет-ресурс URL: https://explainer.ua/shho-take-osint-i-yak-vin-dopomig-vikriti-vbivstva-u-buchi/ (дата звернення: 17.04.2024).

Грянко Анна Георгіївна
студентка 102 БПМС навчальної групи ННІ № 1 НАВС

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

АНАЛІЗ ПРОБЛЕМ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ У ХОДІ ВОЄННОГО ЧАСУ

Інформаційне забезпечення відіграє вирішальну роль під час ведення бойових дій. Своєчасний доступ до достовірної та актуальної інформації є критично важливим для прийняття правильних рішень і досягнення перемоги. Однак у ході війни виникають численні проблеми, пов’язані з інформаційним забезпеченням, які можуть серйозно вплинути на хід бойових дій.

Під інформаційним забезпеченням розуміється комплекс заходів щодо збору, обробки, зберігання, поширення та захисту інформації, необхідної для планування, підготовки та ведення військових операцій. Воно охоплює різноманітні аспекти, починаючи від технічного та програмного забезпечення систем зв’язку та інформаційних мереж і завершуючи підготовкою

висококваліфікованого персоналу, здатного ефективно працювати з величезними масивами даних. Незважаючи на те, що зазначену проблематику вивчали В. Богуш, О. Юдін, Я. Варивода, І. Воробйова, Б. Грушин, Д. Думанський та інші. Проте, порушене питання залишається актуальним.

У сучасних реаліях, коли війни все частіше ведуться не лише на фізичному, а й на інформаційному та кіберпросторі, забезпечення надійного інформаційного супроводу військових дій стає одним із визначальних чинників успіху [1, с. 69]. Проте, на цьому шляху постають численні проблеми та виклики, які необхідно вчасно виявляти та знаходити шляхи їх розв'язання.

Аналізуючи наукові статті та праці науковців виокремлюють такі проблеми:

1. Забезпечення безпеки інформації. Одна з найбільших проблем інформаційного забезпечення під час війни – це забезпечення безпеки інформації. Витік конфіденційних даних може поставити під загрозу безпеку військових операцій, життя солдатів та цивільного населення. Зловмисник може використовувати зазначену інформацію для планування контратак, саботажу чи дезінформації [2, с. 39].

2. Управління великими обсягами інформації. Під час війни генерується величезна кількість інформації з різноманітних джерел, таких як розвідувальні дані, поля бою, цивільні та інші джерела. Управління цими великими масивами даних, їх збір, обробка, аналіз та розповсюдження є складним завданням, особливо в умовах обмеженого часу та ресурсів.

3. Забезпечення достовірності та актуальності інформації. У ході війни інформація може бути спотворена, неповною або застарілою. Дезінформація та пропаганда можуть бути використані противником для введення в оману та дезорієнтації. Забезпечення достовірності та актуальності інформації є критично важливим для прийняття правильних рішень [3, с. 32].

4. Інтеграція різнорідних систем. Сучасні збройні сили використовують різноманітні системи та платформи для збору, обробки та передачі інформації. Інтеграція цих різнорідних систем для забезпечення ефективного обміну інформацією та співпраці є складним завданням.

5. Забезпечення безперервності зв'язку. Під час бойових дій комунікаційні лінії та інфраструктура можуть бути пошкоджені або виведені з ладу. Забезпечення безперервності зв'язку та передачі інформації в таких умовах є критично важливим для координації дій та прийняття рішень [4, с. 167].

Підсумовуючи, слід зазначити, що сучасні війни висувають надзвичайно високі вимоги до систем інформаційного забезпечення та підкреслюють їхню критичну важливість для успішного ведення військових операцій. Серед ключових проблем, що постають на цьому шляху, можна виділити загрози інформаційній безпеці та кібербезпеці, складність управління величезними потоками даних, технічну застарілість наявних систем та недостатню кваліфікацію персоналу.

Для вирішення зазначених проблем необхідно вжити комплекс заходів.

По-перше, потрібно удосконалити законодавче регулювання у сфері інформаційного забезпечення та привести нормативно-правову базу у відповідність із сучасними вимогами. *По-друге*, життєво необхідною є масштабна модернізація технологічної інфраструктури, впровадження новітнього обладнання та програмного забезпечення. *По-третє*, має бути створена єдина універсальна інформаційна система управління ресурсами, яка б об'єднувала всі задіяні у військових діях сили та засоби.

Нарешті, надзвичайно важливим є підвищення кваліфікації персоналу, задіяного в інформаційному супроводженні військових операцій, розширення можливостей для фахового навчання, обміну досвідом та залучення провідних експертів цієї галузі. Лише за умови комплексного підходу до вирішення існуючих проблем можна сподіватися на побудову надійної та дієвої системи інформаційного забезпечення військових дій.

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 [5, с. 106].

Варто розуміти, що виклики у сфері інформаційного супроводження війн будуть постійно зростати у міру розвитку новітніх технологій та еволюції стратегій ведення конфліктів. Тому потрібно не лише швидко реагувати на поточні проблеми, а й розробляти довгострокові перспективні рішення для забезпечення стабільної переваги у цій критично важливій сфері.

Список використаних джерел:

1. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К.: НІСД, 2014. – 328 с.

2. Адміністративно-правове забезпечення інформаційної гігієни під час воєнного стану в Україні / Євген Володимирович Курінний // Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2023. – № 1 (122). – С. 38-43.

3. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи / Оксана Звоздецька // Історико-політичні проблеми сучасного світу. – 2021. – Т. 43.– С. 30-39.

4. Інформаційна безпека людини: теорія і практика: монографія. – Київ: ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

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

Довгалюк Богдан В'ячеславович
слухач магістратури НАВС

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

БЕЗПЕКА В МЕРЕЖІ ІНТЕРНЕТ

1. Загальні принципи:

- *Будьте пильні*: уважно ставтеся до того, на які веб-сайти заходите, що завантажуєте та з ким спілкуєтеся в Інтернеті.
- *Використовуйте надійні паролі*: створіть складні паролі, які відрізняються для різних акаунтів, та не діліться ними з ніким.
- *Установіть антивірусне програмне забезпечення*: оновлюйте його регулярно, щоб захистити пристрій від шкідливого програмного забезпечення.
- *Оновлюйте програмне забезпечення*: регулярно оновлюйте операційну систему та інші програми, щоб усунути вразливості.
- *Будьте обережні з публічною інформацією*: не публікуйте особисту інформацію, таку як адреса, номер телефону чи дата народження, на публічних веб-сайтах або в соціальних мережах.

2. Захист особистої інформації:

- *Уникайте фішингових атак*: не відкривайте підозрілі електронні листи, не переходьте за сумнівними посиланнями та не вводите особисту інформацію на незнайомих веб-сайтах.
- *Звертайте увагу на шифрування*: переконайтеся, що веб-сайти, на яких ви вводите особисту інформацію, використовують шифрування HTTPS.
- *Використовуйте брандмауер*: брандмауер може допомогти захистити ваш комп'ютер від несанкціонованого доступу.
- *Зберігайте конфіденційність паролів*: не зберігайте паролі на комп'ютері та не використовуйте один і той самий пароль для різних акаунтів.

3. Безпека в соціальних мережах:

- *Обмежуйте публічну інформацію*: у налаштуваннях конфіденційності соціальних мереж обмежуйте доступ до вашої особистої інформації.
- *Будьте обережні з друзями*: не додавайте в друзі незнайомців і не діліться особистою інформацією з людьми, яких не знаєте добре.
- *Уникайте кібербулінгу*: не беріть участі в кібербулінгу та повідомляйте про нього, якщо ви його бачите.

- *Звертайтеся за допомогою*: якщо ви стали жертвою онлайн-шахрайства чи кібербулінгу, зверніться за допомогою до дорослого, якому ви довіряєте, або до правоохоронних органів.

4. Безпека дітей в Інтернеті:

- *Спілкуйтеся з дітьми про безпеку в Інтернеті*: поясніть їм, як уникнути онлайн-загроз та як поводитися відповідально в Інтернеті.

- *Використовуйте батьківський контроль*: батьківський контроль може допомогти вам обмежити доступ дітей до певних веб-сайтів і контенту.

- *Будьте зразком для наслідування*: покажіть дітям, як безпечно користуватися Інтернетом, будучи добрим прикладом для них.

- *Створіть атмосферу довіри*: заохочуйте дітей розповідати вам про те, що вони роблять в Інтернеті, щоб ви могли допомогти їм у разі виникнення проблем.

Пам'ятайте: Інтернет може бути чудовим ресурсом, але він також може нести в собі певні ризики. Дотримуючись цих порад, ви можете зробити свій досвід в Інтернеті більш безпечним і приємним.

Драченко Захар Дмитрович
студент 102 БПМС навчальної групи ННІ № 1 НАВС

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

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ СЬОГОДЕННЯ

Протягом історії людства способи розв'язання проблем захисту інформації визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора зазначеної проблеми – комп'ютерні злочини стали характерною ознакою сьогодення.

Незважаючи на те, що проблеми кіберзахисту в Україні були предметом наукових дискусій у роботах: П.П. Андрушка, Ю.М. Батуріна, О.І. Бойцова, О.Г. Волеводза, Б.В. Волженкіна, В.Д. Гавловського, М.В. Гуцалюка, А.М. Жодзішського, В.О. Копилова, Ю.І. Ляпунова, В.Ю. Максимова, О.І. Панфілової, А.М. Попова та інших. В даний час питання кіберзахисту в кіберпросторі є найбільш розповсюдженим і актуальним для суспільства, оскільки питання захисту інформації у мовах сьогодення залишається актуальним.

Проаналізувавши роботи вітчизняних науковців можна резюмувати, що в Україні кіберзлочинність пов'язується передусім із віртуальним простором. Комп'ютерні злочини являють собою передбачені законодавством суспільно небезпечні дії, що посягають на встановлений в суспільстві порядок інформаційних відносин і скоєння їх відбувається з використанням електронно-обчислювальних машин, тобто комп'ютерів, систем та комп'ютерних мереж [1].

Наприклад, на думку Д.П. Біленчука, кіберзлочинністю є злочинність у змодельованому за допомогою комп'ютера інформаційному просторі, в якому перебувають відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді, й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [2, с. 32]. Таке поняття є найбільш адаптованим та наближеним до української кримінально-правової доктрини, оформленої Кримінальним кодексом України [3], але воно не повністю розкриває всю сутність поняття «злочинність».

На думку О.М. Литвака, злочинністю - це відносно масове явище кожного суспільства, що складається з сукупності окреслених кримінальним законом вчинків, вчинених на тій чи іншій території протягом певного часу [4, с. 9].

Таким чином об'єктом злочину зазначених правопорушень виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі, а також комп'ютерна інформація, що обробляється за їх допомогою.

Комп'ютерними злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

У науковій літературі головними причинами комп'ютерних злочинів і пов'язаних з ними викрадень інформації є такі:

– швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;

– широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

– постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць [5, с. 21].

На сьогоднішній день неможливо точно визначити обсяги збитків від комп'ютерних злочинів, але фахівці узгоджують, що ці суми вимірюються мільярдами доларів. Також слід враховувати морально-психологічні наслідки для користувачів, персоналу і власників інформації.

Щодо порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, це може призвести до серйозних наслідків для навколишнього середовища, економіки і безпеки держави, а також здоров'я та навіть життя людей.

У висновку можна сказати, що сучасні технології захисту інформації в умовах сьогодення відіграють критичну роль у забезпеченні безпеки та конфіденційності даних. Слід відзначити, що із зростанням кількості інформації та розвитком цифрових технологій загрози для безпеки даних постійно зростають.

Тому постійне вдосконалення та впровадження новітніх методів захисту стає невід'ємною частиною стратегії будь-якої організації або компанії. Підсумовуючи, ефективна захист інформації вимагає комплексного підходу, що включає в себе як технічні засоби, так і культурні та організаційні заходи. Тільки таким чином можна забезпечити надійну захищеність в умовах сучасного цифрового світу в умовах сьогодення.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 03.04.2024).

2. Біленчук Д. П. Кібрешахраї – хто вони? Міліція України. 1999. № 7–8. С. 32–34.

3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.

4. Литвак О. М. Злочинність, її причини та профілактика. Київ : Україна, 1997. 168 с.

5. Інформаційна безпека комп'ютерних систем і мереж: Методичні вказівки // Укл. А.Ф. Карачка, М.П. Карпінський, А.В. Кулик, Т.В. Лендюк. – Тернопіль: ТАНГ, 2007. – 68 с.

Дубова Аліна Петрівна
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

ПИТАННЯ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ У МЕРЕЖІ ІНТЕРНЕТ В УМОВАХ ВОЄННОГО СТАНУ

У сучасному світі інформаційний простір є невід'ємною складовою суспільства, що визначає його розвиток, взаємодію та сприйняття подій. Однак з поширенням Інтернету і соціальних мереж наш інформаційний ландшафт став набагато складнішим і вразливішим до маніпуляцій та дезінформації. Особливо актуальним це стає в умовах воєнного стану, коли зловживання інформацією може мати серйозні наслідки для національної безпеки та стабільності.

Питання протидії дезінформації в мережі Інтернет в умовах воєнного стану є одним із найважливіших завдань для сучасного суспільства. Швидкість поширення та доступність інформації у віртуальному просторі дозволяють дезінформаторам легко впливати на громадську думку, маніпулювати переконаннями та формувати негативне сприйняття подій.

Незважаючи на те, що теоретичні та практичні аспекти пов'язані з питаннями протидії дезінформації були предметом досліджень у роботах І. Гирича, Б. Гуменюка, Л. Масенка, В. Огнев'юка, В. Огризка, О. Палія, В. Піскун, П. Полянського, К. Ярового та інших, зазначена проблематика залишається актуальною та потребує подальших досліджень. Тому деякі аспекти вимагають більш детального аналізу.

Слід зазначити, що дезінформація визнається як очевидно неправдива або така, що призводить до оману, і має дві основні характеристики [1]. По-перше, вона створена, поширена або представлена з метою отримання фінансової вигоди або з умислом введення громадськості в оману. Друга характеристика полягає в тому, що дезінформація може завдати шкоди суспільству шляхом загрози демократичним процесам, процесам формування політики, а також суспільним благам, таким як захист здоров'я громадян, довкілля та безпека. У тому числі дезінформація може бути поширена через соціальні мережі, новинні сайти, блоги або інші онлайн-платформи і може створювати плутанину та спричиняти шкоду суспільству.

Дослідник Х. Фокс надає поняття дезінформації, звужене до дій окремих акторів: дезінформація - це «інформація, що навмисно вводить в оману, яка оголошена публічно чи стала предметом витоку інформації з боку уряду чи розвідки» [2, с. 13].

Пропаганда передбачає поширення із використанням маніпулювання будь-якої інформації (правдивої, неправдивої, спотвореної) з метою формування у певної цільової аудиторії необхідних думок, мотивів, поглядів, ставлень, устремлінь. Вона впливає на інтелектуальну сферу, психоемоційний стан, мотиви та поведінку людей й вирізняється цілеспрямованістю (мета, система, структурованість), масовістю (зорієнтованістю на широке коло людей – велика цільова аудиторія), нівелюванням критичності мислення (некритичне сприйняття інформації, що зумовлює безапеляційну віру у все почуте/побачене), дозованістю (підбирається та використовується тільки та інформація, яка відповідає меті і особливостям цільової аудиторії).

Наприклад, Г.Г. Почепцов виділяє три основі етапи пропагандистської комунікації:

- переорієнтація громадської думки шляхом провадження нових цінностей;
- економічна дезінформація;
- розповсюдження моделей кращого життя через засоби масової інформації, кіно та інші культурні засоби.

На його думку, пропагандистський вплив здатний створювати прийнятний для громадян уявлення про майбутнє, однак, отримані результати часто не відповідають дійсності [3, с. 57].

На законодавчому рівні під дезінформацією слід розуміти створення, поширення, використання відомостей, що відноситься до дезінформації, що може та/або викликає паніку серед населення та/або уводить в оману [4].

У тому числі, слід зауважити, що з перших днів початку повномасштабної війни окупанта у Національній академії внутрішніх справ організовано робочу Telegram-групу «АнтиОрк», направлену на інформаційне протистояння ворогу у кіберпросторі:

- розповсюдження фото- та відео- матеріалів, розсилка статей про військові злочини країни-агресорки на території України у соціальних мережах (Twitter, Instagram, TikTok);
- •створення постів на російських платформах про заклик мешканців російських міст щодо створення петицій про повалення тоталітарного кремлівського режиму та негайного припинення окупаційних військових дій в Україні;
- •дії, направлені на пошук і збір інформації щодо переміщення військової ворожої техніки, диверсійно-розвідувальних груп, ворожих планів, корегування артилерією;

• •видалення з геопозицій «фейкових» міток для нанесення ракетних, авіаційних та артилерійських ударів з мап Google та Яндекс;

• •висвітлення реалій війни на Україні з боку агресора у форматі відеороликів на наших каналах (TikTok, YouTube) [5, с. 352-353].

Крім того дезінформація може бути використана з метою маніпулювання думками та переконаннями користувачів. Це може стати серйозною проблемою в політичних кампаніях, коли неправдива інформація може вплинути на вибір виборців та результати виборів. Також, дезінформація може мати серйозні наслідки в різних галузях, наприклад, в медицині чи науці, де неправильна інформація може призвести до небезпечних результатів і навіть загрожувати життю людей. Наприклад, неправильна інформація про вакцини може призвести до того, що люди не будуть вакцинуватися проти захворювань, що може призвести до поширення хвороб та смертей.

Своєю чергою, Дубов Д.В. вважає, що проблема дезінформації в соціальних мережах є актуальною та важливою, оскільки вона може впливати на різні сфери нашого життя, такі як політика, економіка, наука, медицина і т.д. Одна з найбільших проблем, пов’язаних з дезінформацією в соціальних мережах, полягає у тому, що вона швидко поширюється та може досягати широкої аудиторії. Зазначене стає можливим завдяки алгоритмам соціальних мереж, які визначають, яка інформація відображається у стрічці новин користувачів. Оскільки ці алгоритми часто базуються на популярності контенту та інших факторах, таких як коментарі та лайки, то дезінформаційний контент може виявитися більш «цікавим» для алгоритмів, ніж достовірна інформація [6, с. 77].

Шлапаченко В.М. вважає, що протидія дезінформації в соціальних мережах - це складний процес, що вимагає спільних зусиль користувачів, соціальних мереж та держави. Користувачі повинні бути свідомі того, що інформація, яку вони отримують в соціальних мережах, може бути дезінформацією, тому вони повинні перевіряти джерело інформації та шукати додаткові докази перед тим, як відправляти її далі [7, 84].

Однак, на мою думку під дезінформацією у мережі Інтернет слід розуміти, що це поширення неправдивої, маніпулятивної або вигаданої інформації з метою введення в оману аудиторії або досягнення певних цілей, таких як політична маніпуляція, фінансова вигода або психологічний вплив.

Отже, на підставі вищевикладеного слід зробити наступні висновки, що використання інформаційних ресурсів створює нові виклики у сфері засвоєння інформації та розвитку медійної грамотності. Важливо розвивати критичне мислення та здатність аналізувати інформацію з різних джерел перед прийняттям рішень. На нашу думку, необхідно вдосконалювати механізми виявлення та протидії дезінформації, сприяючи формуванню об’єктивного уявлення про події та явища в суспільстві.

Крім цього, важливо розглянути розробку реальної моделі для оцінки наслідків дезінформації та її практичне застосування. Зазначене допоможе переконати громадян у необхідності володіння медіаграмотністю у демократичному та розвиненому суспільстві, не лише як інтелектуальний тренд, але й як важливу життєву навичку.

Список використаних джерел:

1. Деякі питання адаптації законодавства України до законодавства Європейського Союзу: Постанова Кабінету Міністрів України від 15.10.2004 р. № 1365// Офіційний вісник України від 05.11.2004. – 2004р., № 42, стор. 35, ст. 2763.

2. Fox C. J. Information and misinformation. Westport, CT: Greenwood Press, 2011. Pp. 12–15.

3. Почепцов Г. Г. Смисли і війна. Україна і росія в інформаційні та смисловій війні. Київ, 2016. 151 с.

4. Офіційний сайт Центру протидії дезінформації при РНБО України: Глосарій: механізми. URL: https://cpd.gov.ua/category/glossary/mechanisms/ (Дата звернення: 31.03.2024).

5. Яровий К. В. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. Всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. 618 с.

6. Дубов Д. В. Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики? Київ: ТОВ «Видавництво Сталь», 2019. 254 с.

7. Шлапаченко В. М. Дезінформація як спосіб інформаційно-психологічного впливу. Інформаційна безпека людини, суспільства, держави. 2013. № 2(12). С. 78–86. URL: http://nbuv.gov.ua/UJRN/ iblsd_2013_2_15 (дата звернення: 31.03.2024).

Жмуровська Катерина Романівна
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ

Науковий керівник:
Грищенко Денис Олександрович
старший викладач кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, підполковник поліції

ВПЛИВ ДЕЗІНФОРМАЦІЇ НА ГРОМАДСЬКУ ДУМКУ ТА ПОВЕДІНКУ В УМОВАХ ВОЄННОГО КОНФЛІКТУ

В умовах воєнного конфлікту дезінформація набуває особливого значення, відіграючи важливу роль у формуванні громадської думки та впливаючи на поведінку людей. У цьому контексті, розуміння сутності та механізмів дезінформації стає надзвичайно актуальним. Дезінформація, часто прихована під покровом правдивої інформації, здатна маніпулювати сприйняттям подій, формуючи стереотипи та розпалюючи паніку та страх. У цьому вступі ми розглянемо вплив дезінформації на громадську думку та поведінку в контексті воєнного конфлікту, а також проаналізуємо шляхи протидії цьому явищу.

У світлі військових дій, дезінформація виконує важливу місію у створенні образу ворога та інтерпретації подій. За допомогою маніпуляційних прийомів та підбору фактів, що сприймаються з певного ракурсу, дезінформація перетворює неправдиву чи неповну інформацію на засіб впливу на громадську думку. Вона формує уявлення про супротивника, відбиваючи його у світлі загрози та зла, що сприяє розширенню ворожнечі та підтримує дух бойового патріотизму.

Ми живемо в столітті високих інформаційних технологій, завдяки чому щодня отримуємо величезну кількість нової інформації, іноді навіть не замислюючись, що її джерело – інтернет, телебачення, радіо, реклама – щоденно впливає на формування у нас певних соціальних стереотипів, які в свою чергу визначають нашу поведінку, моральні норми, ставлення до навколишнього світу, формують політичні, релігійні та світоглядні концепції [1].

Створюючи стереотипи та перекручуючи факти, дезінформація здатна перетворити непротилежних сторін конфлікту в абсолютних героїв або злочинців. Це може призвести до прискорення процесу розпалювання ворожнечі та обґрунтування воєнних дій, адже образ ворога, який створюється за допомогою дезінформації, сприймається як загроза, що потребує термінової реакції.

Також, дезінформація часто використовується для поширення паніки та страху серед населення. Популяризуючи негативні сторони воєнних дій або збільшуючи розмір загрози, вона створює атмосферу невпевненості та хаосу, що сприяє паніці та недовірі до власної держави. Це може мати серйозні наслідки для ефективності ведення війни та стабільності суспільства в цілому.

У військовому конфлікті дезінформація виступає як потужний інструмент, що впливає на поведінку громадськості, викликаючи реакції, які можуть мати вирішальне значення для результатів конфлікту.

Маніпуляція масовими медіа – один із основних методів, що використовуються для впливу на поведінку громадськості. Подача дезінформації через телебачення, радіо, Інтернет та інші масові засоби зв’язку може змінити сприйняття подій та переконання громадян, що може вплинути на їхні дії та реакції.

Найбільшу роль у формуванні й поширенні громадської думки відіграють медіа. Медіа не тільки інформують, повідомляють новини, але й пропагують певні ідеї, погляди, вчення, політичні програми і беруть участь у соціальному управлінні. Таким чином, медіа підштовхують людину до певних вчинків, дій шляхом формування громадської думки, вироблення певних соціальних установок, формування переконань [2].

Поглиблення розділених думок та ворожнечі – дезінформація також може призвести до подальшого роз’єднання суспільства та збільшення конфліктів між різними соціальними групами. Вона може підживлювати існуючі ворожнечі, розпалювати пристрасть та підтримувати кшталт враження "ми проти них", що загострює соціальні та політичні розбіжності.

Збентеження та зниження довіри до інформаційних джерел – внаслідок поширення дезінформації може виникнути загальне збентеження серед громадськості та сумніви у достовірності інформації. Це може призвести до зниження довіри до різних джерел інформації, включаючи як офіційні, так і альтернативні медіа, що ускладнює процес прийняття обґрунтованих рішень та сприяє загальній дезорієнтації громадськості.

У зламіні дезінформації важливо розробити та впровадити ефективні стратегії, спрямовані на захист громадської думки та поведінки. Для цього можна використовувати такі підходи:

Збільшення інформаційної грамотності громадян – розвиток навичок критичного мислення та аналізу інформації може допомогти громадянам відрізняти дезінформацію від правдивої інформації. Просвітницькі кампанії, тренінги та освітні програми можуть допомогти зробити громадян менш вразливими до маніпуляційних прийомів дезінформації.

Посилення ролі незалежних медіа – підтримка незалежних та об’єктивних медіа організацій може стати ключовим чинником у боротьбі з дезінформацією.

Забезпечення доступу до різноманітної інформації та розслідування фактів може допомогти зменшити вплив маніпуляційних медіа на громадську думку.

Ми, на жаль, є свідками наслідків пропаганди та інформаційної війни. Важливість свідомого споживання інформації вже не потребує доведення, зокрема: запобігання потраплянню в інформаційну бульбашку, яку створюють алгоритми соцмережі; перевірка об'єктивності інформації, розрізнення фактів і суджень; прийомів маніпуляції громадською думкою; навичок послуговуватися офіційними джерелами інформації, вміння обирати медіа, які дотримуються журналістських стандартів, таких як об'єктивність, баланс думок тощо. Саме тому медіа-освіта громадян – це наразі частина стратегії інформаційної безпеки України [3].

Використання технологій для виявлення та припинення дезінформації – розробка та використання алгоритмів машинного навчання та штучного інтелекту може допомогти виявляти та відстежувати поширення дезінформації в мережі. Також важливо співпрацювати з провайдерами соціальних мереж та інших онлайн-платформ для припинення поширення шкідливої інформації.

Ці підходи можуть сприяти зменшенню впливу дезінформації на громадську думку та поведінку в умовах воєнного конфлікту, забезпечуючи більш об'єктивне та інформоване суспільство.

У світлі аналізу впливу дезінформації на громадську думку та поведінку в умовах воєнного конфлікту стає очевидним, що це явище є надзвичайно складним і важливим для суспільства в цілому. За допомогою дезінформації може створюватися не лише образ ворога та викривлене сприйняття подій, але й маніпулювати поведінкою мас. Значення протидії дезінформації в умовах воєнного конфлікту набуває величезної важливості. Посилення інформаційної грамотності, підтримка незалежних медіа та використання сучасних технологій є ключовими складовими успішної стратегії протидії дезінформації.

Питання, що стоять перед дослідниками та громадськістю, щодо виявлення та подолання дезінформації в умовах воєнного конфлікту, залишаються відкритими. Подальші дослідження цього питання можуть допомогти розробити більш ефективні стратегії протидії та забезпечити більш стійке та інформоване суспільство.

Список використаних джерел:

1. Створення стереотипів засобами масової інформації в добу інформаційного суспільства. URL: http://publications.lnu.edu.ua/collections/index.php/teleradio/article/viewFile/678/683.

2. Вплив медіа на формування громадської думки у світі. URL: https://philol.vernadskyjournals.in.ua/journals/2021/1_2021/part_3/52.pdf.

3. Медіаінформаційна грамотність громадян як вимога сьогодення. Роль ЗМІ в інформаційному просторі. URL: https://umoloda.kyiv.ua/number/3880/188/179363.

Забаштанський Андрій Андрійович
студент 202_СПД навчальної групи ННІ № 3 НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СИТУАЦІЙНИХ ЦЕНТРІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Наказом МВС України від 27 квітня 2020 року № 357 затверджена Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України (далі – НПУ) [1, 2]. Відповідно до п. 2 розділу І зазначеної Інструкції під *оперативним інформуванням* розуміють єдину систему збирання, опрацювання та подання до чергової служби вищого рівня інформації про правопорушення або подію з метою організації контролю за встановленням і затриманням осіб, які вчинили кримінальні правопорушення, а також оперативного реагування на надзвичайні ситуації. При цьому заяви і повідомлення про правопорушення або події працівниками чергової служби органів (підрозділів) поліції реєструються в інформаційній підсистемі «Єдиний облік» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» [3, 4].

З метою забезпечення належного функціонування зазначеної єдиної системи збирання, опрацювання та подання до чергової служби вищого рівня інформації про правопорушення або подію використовується інтегрована інформаційна *система оперативного інформування* (далі – СОІ) НПУ, яка є подальшим розвитком автоматизованої СОІ Міністерства внутрішніх справ України, створеної протягом 1992-2015 років [5, 6].

НПУ вживає заходи для організації належного інформаційно-аналітичного забезпечення своєї діяльності, у тому числі функціонування СОІ. Одним з них є впровадження Ситуаційних центрів (далі – СЦ) [7]. СЦ – це сучасна форма організації аналітичної діяльності, яка базується на синтезі інформаційно-комунікаційних технологій, засобів накопичення і представлення інформації, комп’ютерних засобів підтримки прийняття рішень [8].

СЦ – це підрозділ зі збору, обробки та аналізу інформації про рівень, структуру і динаміку злочинності по всій Україні. Існує Ситуаційний центр НПУ, де проводиться тільки збір і обробка інформації, а також СЦ в місті Києві та областях, в складі яких працює і служба «102» [7]. Основні проблеми впровадження ситуаційних центрів в органах Національної поліції України та перспективи їх розвитку розглянуто в роботах [9-12]. Питанням впровадження можливостей «розумних камер» в діяльність СЦ НПУ присвячена стаття [13], а можливості СЦ НПУ щодо виявлення та розкриття злочинів розглянуто в роботі [14].

В умовах воєнного стану змін у повноваженнях, компетенції, правах та обов'язках, порядках та процедурах зазнають майже всі державні інституції. Про зміни до нормативно-правових актів, які регулюють функціонування НПУ в період воєнного стану, зазначено в роботі [15]. Особливості в умовах війни стану оперативної обстановки в країні та діяльності органів НПУ відображено в інтерв'ю Голови Національної поліції України Івана Вигівського [16], а саме:

1) від початку повномасштабного вторгнення росії на територію України простежується тенденція до зменшення кількості звернень до поліції в регіонах, які опинилися в зоні бойових дій, та, навпаки, у регіонах, куди тоді переїхало чимало людей, кількість вчинених правопорушень трохи зросла;

2) у цілому по країні, завдяки запровадженню комендантської години, збільшенню присутності на вулицях населених пунктів поліцейських, військових, нацгвардійців, представників добровольчих формувань територіальних громад, а також обмеженням продажу алкогольної продукції, зменшився рівень вуличної злочинності, зокрема розбоїв і грабежів;

3) під час війни збільшилось на 50 % кількість поліцейських, що заступає на добове чергування, в тому числі на патрулювання вулиць;

4) посилення в березні 2022 року Верховною Радою України відповідальності за вчинення в умовах воєнного стану низки майнових злочинів також певною мірою стало стримувальним чинником для деяких злочинців;

5) загальна реєстрація злочинів збільшилась, у тому числі за рахунок воєнних злочинів (спостерігається масове вчинення військовослужбовцями збройних сил країни агресора воєнних злочинів);

6) війна продовжує впливати на динаміку окремих видів злочинів, зокрема тяжких та особливо тяжких, загальна кількість яких зросла;

7) окремими видами кримінальних правопорушень, які набули більшого поширення в умовах війни, є шахрайства;

8) незважаючи на зростання за певний період часу у порівнянні з минулим роком кількості злочинів на 57 %, кількість розкритих злочинів також збільшилась на 71 %, більше справ спрямовано до суду на 67 %;

9) у подальшому планується поєднати в єдину інтеграційну систему всі камери відеонагляду в державі;

10) досить ефективно працює кримінальний аналіз. Цей підрозділ також працює і на базі Центру "112", який був нещодавно відкритий міністром внутрішніх справ України Ігорем Клименком у місті Києві, перший в Україні. Там же ситуаційний центр реагування, де наряду з поліцією постійно перебувають працівники Державної служби з надзвичайних ситуацій, Національної гвардії України та Державної прикордонної служби.

Безумовно, зазначене вплинуло на особливості виконання основного завдання СЦ – забезпечення координації та управління силами і засобами поліції в разі ускладнення оперативної обстановки або виникнення надзвичайних ситуацій [17]. Тому аналітики СЦ НПУ постійно збирають і обробляють відповідну інформацію, групують і передають її Голові НПУ для своєчасного прийняття відповідних управлінських рішень.

При цьому аналітики використовують три види аналізу [17]:

1) *стратегічний (кримінологічний)* – це аналіз злочинності, її рівня, поширеності, динаміки, структури загалом; результати роботи розглядаються під час засідань колегії, підбиття підсумків;

2) *тактичний* – це ситуація впродовж доби, тижня щодо конкретних регіонів, конкретних видів злочинів;

3) *практичний* – це оперативний кримінальний аналіз по кожному конкретному тяжкому та особливо тяжкому злочину.

Необхідно відмітити, що аналітики СЦ НПУ, крім щоденного зведення за добу, також готують звіти за тиждень і за місяць.

В обласних СЦ оператори служби «102» приймають всі звернення громадян, передають інформацію диспетчерам, які, в свою чергу, направляють наряди поліції на виклики і контролюють їх виконання. Резонансна подія, яка відбувається в будь-якій точці країни, майже миттєво з’являється на моніторах чергової частини Ситуаційного центру НПУ [14].

Висновки: проведений нами аналіз літературних джерел щодо функціонування Ситуаційних центрів НПУ за останні роки свідчить про важливість результатів їх роботи, особливо в умовах воєнного стану, для забезпечення органами Національної поліції контролю криміногенної ситуації в країні та відповідного реагування на неї, а також у повоєнний стан не допущення дестабілізації та підвищення рівня злочинності в країні.

Список використаних джерел:

1. Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України: Наказ МВС України від 27 квіт. 2020 р. № 357. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text (дата звернення: 16.04.2024).

2. Про Національну поліцію: Закон України від 02 лип. 2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.

3. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 14 черв. 2019 р. № 508. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0739-19#Text (дата звернення: 16.04.2024).

4. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення: 16.04.2024).

5. Функціонування системи оперативного інформування МВС України / [В. А. Кудінов, П. П. Артеменко, О. В. Золотар та ін.]; за ред. В. А. Кудінова. Спеціальна техніка. Загальна частина: посіб. Київ: Київський нац. ун-т внутр. справ, 2007. С. 156–172.

6. Кудінов В. А. Становлення, сучасний стан і перспективи розвитку автоматизованої системи оперативного інформування МВС України про резонансні злочини та інші надзвичайні події. Бюлетень з обміну досвідом роботи МВС України. 2012. № 190. С. 9–27.

7. Кудінов В. А. Удосконалення функціонування системи оперативного інформування Національної поліції України шляхом створення Ситуаційних центрів. Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (Дніпро, 23 листоп. 2018 р.). Дніпро: Дніпропетровський держ. ун-т внутр. справ, 2018. С. 44–46.

8. Поняття Ситуаційного центру. URL: http://inmad.vntu.edu.ua/portal/static/952500A7-287E-4743-A7B1-0B8C1105B2CA.pdf (дата звернення: 16.04.2024).

9. Кудінов В. А. Проблеми впровадження ситуаційних центрів в органах Національної поліції України. Сучасні проблеми правового, економічного та соціального розвитку держави: матеріали VII міжнар. наук.-практ. конф. (Харків, 30 листоп. 2018 р.). Харків: Харківський нац. ун-т внутр. справ, 2018. С. 143–145.

10. Кудінов В. А. Правове та організаційне забезпечення інформаційної безпеки у діяльності Ситуаційного центру Національної поліції України. Інформаційна безпека в діяльності поліції: матеріали наук.-практ. семінару (Кривий Ріг, 03 квіт. 2020 р.). Кривий Ріг: Донецький юрид. ін-т МВС України, 2020. С. 74–78.

11. Кудінов В. А. Основні показники оцінки надійності функціонування апаратно-програмних засобів Ситуаційних центрів Національної поліції України. Кібербезпека в Україні: правові та організаційні питання: матеріали ІІ міжнар. наук.-практ. конф. (Одеса, 26 листоп. 2020 р.). Одеса: Одеський держ. ун-т внутр. справ, 2020. С. 59–61.

12. Кудінов В. А. Сучасний стан та перспективи розвитку Ситуаційних центрів Національної поліції як складової сектору національної безпеки і оборони України. Стан та перспективи реформування сектору безпеки і оборони України: матеріали II міжнар. наук.-практ. конф. (Київ, 30 листоп. 2018 р.). Київ: Київський нац. ун-т імені Тараса Шевченка, 2018. С. 317–318.

13. Кудінов В. А. Впровадження можливостей «розумних камер» в місті Києві в діяльність Ситуаційних центрів Національної поліції України. Інформаційні технології в культурі, мистецтві, освіті, науці, економіці та бізнесі: матеріали міжнар. наук.-практ. конф. (Київ, 18-19 квіт. 2019 р.). Київ: Київський нац. ун-т культури і мистецтв, 2019. Ч. 2. С. 248–250.

14. Кудінов В. А. Можливості Ситуаційних центрів Національної поліції України щодо виявлення та розкриття злочинів. Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід: матеріали міжнар. наук.-практ. круглого столу (Київ, 19 лют. 2020 р.). Київ: Нац. акад. внутр. справ, 2020. С. 106–109.

15. Національна поліція в умовах воєнного стану: зміни в законодавстві. Law-in-War: [сайт]. URL: https://law-in-war.org/naczionalna-policziya-v-umovah-voyennogo-stanu-zminy-v-zakonodavstvi/ (дата звернення: 16.04.2024).

16. Бодня Т. Голова Національної поліції Іван Вигівський: «Війна продовжує впливати на динаміку окремих видів злочинів, зокрема тяжких та особливо тяжких». Цензор.НЕТ: [сайт]. URL: https://censor.net/ua/resonance/3437662/golova_natsionalnoyi_politsiyi_ivan_vygivskyyi_viyina_prodovjuye_vplyvaty_na_dynamiku_okremyh_vydiv (дата звернення: 16.04.2024).

17. Основні завдання та функції Ситуаційних центрів органів Національної поліції. Prezi: [сайт]. URL: https://prezi.com/p/zhigbbcnpwj5/presentation/ (дата звернення: 16.04.2024).

Замула Дар'я Володимирівна
студентка 102 БПМС навчальної групи ННІ №1 НАВС

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

ПРОБЛЕМИ ЗАХИСТУ ДАНИХ У МЕРЕЖІ-ІНТЕРНЕТ В УМОВАХ ВОЄННОГО СТАНУ

У світі, де віртуальна реальність все більше переплітається з реальним життям, проблеми захисту даних у мережі Інтернет набувають надзвичайної актуальності. Швидкість технологічного розвитку призводить до появи нових загроз та викликів для конфіденційності та приватності інформації в онлайн середовищі. У цьому контексті розгляд проблем захисту даних стає невід'ємною складовою наукового дослідження, оскільки від нього залежить забезпечення безпеки користувачів та надійність інформаційних систем. В даній статті ми дослідимо актуальні аспекти цієї проблематики та запропонуємо шляхи її вирішення в умовах сучасного цифрового світу.

Захист даних, захист інформації – це сукупність заходів і відповідних засобів, які забезпечують захист прав власності власників інформаційної продукції, у першу чергу – програм, баз і банків даних від несанкціонованого доступу, використання, руйнування або завдання шкоди в будь-якій іншій формі [1, с. 78].

У галузі знань із захисту інформації сформульовано такі основні твердження:

1) абсолютно надійний захист створити неможливо. Система захисту інформації може бути, в кращому разі, адекватною потенційним загрозам;

2) система захисту інформації повинна бути комплексною: слід використовувати не тільки технічні засоби захисту, а й адміністративні та правові;

3) система захисту інформації повинна бути гнучкою, здатною адаптуватися до умов, що змінюються.

Виходячи з можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації існують множинні види захисту, які можна поділити на такі умовні групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

На думку Виганяйло С.М., під правовими засобами захисту слід розуміти, чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання інформаційних технологій [2, с. 38].

Адміністративні (організаційні) заходи забезпечення безпеки інформації визначають правила та процедури, що регулюють роботу інформаційної системи, використання її ресурсів та діяльність персоналу. Вони також визначають способи взаємодії користувачів із системою з метою ускладнення або запобігання порушенням безпеки. Адміністративні заходи охоплюють:

1) розмежування доступу до інформації за допомогою паролів, профілів повноважень тощо; розроблення адміністративних норм та системи покарань за їх порушення тощо);

2) розроблення правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією);

3) заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань, тощо);

4) заходи, які передбачаються під час проектування, будівництва та облаштування об’єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль працівників тощо);

5) заходи, що вживаються під час проектування, розроблення, ремонту й модифікації обладнання та програмного забезпечення (перевірка на відповідність стандартам всіх технічних і програмних засобів, строге затвердження, оцінка та ухвалення будь-яких змін) [3, с. 138].

Адміністративні засоби захисту інформації є важливим елементом, оскільки вони можуть доповнювати законодавчі норми та застосовуватися у випадках, коли потрібно забезпечити безпеку організації. Часто вони передбачають використання інших видів захисту, таких як технічний чи програмний, що забезпечує більш надійний рівень захисту. Проте велика кількість адміністративних правил може ускладнювати роботу працівників і навіть знижувати ефективність захисту, оскільки інструкції можуть залишатися невиконаними [4, с. 216].

Проблематика полягає в тому, що надмірна кількість адміністративних правил у сфері захисту інформації може призвести до недоліків у роботі персоналу та зниження ефективності заходів безпеки. Відповідно, це може стати загрозою для безпеки інформації, оскільки інструкції можуть бути ігнорованими або виконуватися неадекватно через їх велику кількість.

Надмірна адміністративна складність може призвести до витрат часу та ресурсів на виконання процедур, що не завжди може бути обґрунтованим з точки зору реальних загроз безпеці.

Таким чином, забезпечення захисту даних та інформації є важливим аспектом у сучасному світі. У зв'язку з цим, існує ряд різноманітних методів захисту даних, які можна класифікувати на кілька основних категорій: правові, адміністративні, технічні та програмні. Кожен з цих підходів спрямований на захист даних та інформації від несанкціонованого доступу, використання та руйнування.

Список використаних джерел:

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

2. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 108 с.

3. Іванов В. Г. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посіб. / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.; за заг. ред. В. Г. Іванова. – Х.: Право, 2010. – 240 с.

4. Вишня В. Б. Інформаційні технології: навч. підручник / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро: ДДУВС, 2020. 418 с.

Іваненко Катерина Володимирівна
студентка 102 БПМС навчальної групи ННІ № 1 НАВС

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

ОПТИМІЗАЦІЯ РОБОТИ СИСТЕМИ «ЦУНАМІ» В ПРАВООХОРОННИХ ОРГАНАХ

Системи централізованого управління нарядами поліції є важливим елементом забезпечення громадського порядку та безпеки в сучасних містах. Однак, у зв'язку з постійними змінами у соціальному, технологічному та кримінальному середовищі, необхідність постійного вдосконалення цих систем стає невідкладною. Особливо в контексті великих міст, де складність та обсяги завдань, що стоять перед правоохоронними органами, постійно зростають.

Система централізованого управління нарядами поліції (скорочено – система «ЦУНАМІ») являє собою комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами Національної поліції.

Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них [1, с. 81]. Аналізуючи організаційно-контролюючу частину програмного комплексу «ЦУНАМІ», слід зазначити, що для інформаційного забезпечення патрульної поліції використовується програмний комплекс «ЦУНАМІ», який можна розділити на дві основні складові – організаційно-контролюючу та інформаційно-пошукову [2].

Наприклад, патрульна поліція виконує функції підрозділу швидкого реагування у протидії із кримінальними та адміністративними правопорушеннями, вона повинна якнайшвидше прибувати на місце події. Час реагування на подію, як правило, складається з трьох етапів:

1) приймання повідомлення у Call-центрі (служба « 102»);

2) обробка диспетчером інформації за карткою «102» та складання завдання для найближчого вільного патруля;

3) прийом завдання, прибуття на місце та реагування поліцейськими на подію [3, с. 147].

Однак, як показують проведені дослідження, найбільш проблемною ділянкою у цьому ланцюжку є служба «102»:

- Оператори часто не якісно та повільно збирають первинні відомості щодо події. Зазначене пояснюється відсутністю мотивації працівників Call-центру, посади яких комплектуються за остаточним принципом, та як правило, з поліцейських, посади яких скорочені.

- Програмне забезпечення Call-центру «ЦУНАМІ» розроблено для цифрових телефонних станцій, відсутність якої в управліннях поліції обмежує можливості оболонки «102» щодо онлайн інформації про заявника та швидкості оформлення картки «102».

- Заповнена картка надсилається диспетчеру та черговому відділу поліції за місцем відбування події для занесення у спеціальні обліки. Диспетчер виконує функції організаційно-інформаційного супроводження діяльності патрульної поліції і є дуже важливим елементом ефективності роботи.

На нашу думку, необхідно забезпечити патрулі більшою інформаційною підтримкою від диспетчерів, які отримали доступ до ІПС Національної поліції України. Експерименти, проведені у Департаменті патрульній поліції м. Києва, показали, що надання найбільш підготовлених патрульних диспетчерам значно підвищує ефективність їхніх дій [3, с. 217]. Зазначене дозволяє оптимізувати роботу патрулів та зменшити час реагування на надзвичайні події.

Крім цього, патрульні поліцейські стикаються з численними проблемами у роботі з системою централізованого управління нарядами поліції «ЦУНАМІ». Ці проблеми включають системні збої під час реєстрації нових змін патрульних, особливо при одночасних змінах у всіх містах України, а також відсутність зв'язку з мобільним оператором «Київстар». Збільшення об'єму інформаційних потоків, шифрування інформації та перевантаженість стільникових мереж також ускладнюють ситуацію. Вирішенням цих проблем може бути надання пріоритету сім-карткам «Київстару», встановленим у планшетах з «ЦУНАМІ», а також реалізація функції «Голосового набору» для складання звітів. Патрульні також вимагають покращення нормативно-правової підтримки їхньої діяльності в системі «ЦУНАМІ» [4, с. 183].

Тому усунення технічних проблем, пов'язаних з GPS-навігатором та технічною підтримкою мобільного оператора, а також забезпечення доступу до повної інформації в базах даних щодо осіб, речей та транспортних засобів у розшуку, є нагальними завданнями. Крім того, важливо розмістити фототеку на захищеній мобільній частині системи «ЦУНАМІ», щоб уникнути можливого витоку службової інформації.

В.Б. Вишня вважає, що система «ЦУНАМІ» потребує оптимізації для підвищення ефективності та безпеки. Недоліком є обмежена можливість диспетчера відстежувати дії патрульного під час виконання завдань, що ускладнює контроль та втручання у роботу наряду. Пропонується введення нових зв'язків елементів системи, що дозволить диспетчеру оперативно отримувати інформацію про події через відеореєстратор патрульного [5, с. 113-114]. Вважаємо, що зазначене забезпечить реальний контроль та можливість оперативного втручання диспетчера, підвищуючи ефективність та безпеку діяльності патрульного наряду.

Вищевикладене підтверджує, що комплекс «ЦУНАМІ» є надзвичайно ефективним засобом для організаційного та інформаційного забезпечення реагування підрозділів Національної поліції на події. Електронна картка реагування на подію, що є частиною цієї системи, покращує якість збору та фіксації первинної інформації на місцях подій, мінімізуючи ризик корупційного впливу на неї. Забезпечення правоохоронцям швидкого та зручного доступу до комунікаційних баз даних є ще одним важливим аспектом зазначеної системи.

Список використаних джерел:

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

2. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ МВС України від 03.08.2017 № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

3. Вишня В. Б. Інформаційні технології: навч. підручник. / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро : ДДУВС, 2020. 418 с.

4. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності: навч. посіб. Дніпро : ДДУВС, 2018. 218 с.

5. Вишня В. Б. Удосконалення системи управління нарядами мобільної патрульної служби Національної поліції України. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2017. № 2. С. 113-116.

Ігонін Олександр Євгенович
слухач магістратури НАВС

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, капітан поліції

БЕЗПЕКА КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

Першим і найважливішим кроком до забезпечення безпеки вашої електронної скриньки є створення міцного пароля. Безпека починається зі створення надійного пароля. Надійний пароль – це пароль, який:

- Щонайменше 12 символів, але краще 14 символів.
- Комбінація букв у верхньому регістрі, букв нижнього регістра, чисел і символів.
- Це не слово, яке можна знайти у словнику або ім’я особи, символу, продукту чи організації.
- Значно відрізняється від попередніх.

Легко запам’ятати вас, але іншим користувачам складно вгадати. Рекомендовано використовувати таку пам’ятну фразу, як "6MonkeysRLooking^".Створивши надійний пароль, дотримуйтеся наведених нижче рекомендацій, щоб захистити його.

- Нікому не передавайте пароль. Це стосується навіть друзів і членів сім’ї.
- Ніколи не надсилайте пароль електронною поштою, у миттєвому повідомленні або за допомогою інших засобів зв’язку, які не гарантують надійного захисту.

- Використовуйте унікальний пароль для кожного веб-сайту. Якщо краде відомості облікового запису з одного сайту, вони намагатимуться використовувати ці облікові дані на сотнях інших відомих веб-сайтів, таких як банківські послуги, соціальні мережі або покупки в Інтернеті, сподіваючись, що пароль повторно використовується в іншому місці. Це називається "Атака, яка має облікові дані", і вона дуже поширена.
- Якщо ви не хочете запам’ятовувати декілька паролів, скористайтеся диспетчером паролів. Найкращі диспетчери паролів будуть автоматично оновлювати збережені паролі, зберігати їх у зашифрованому вигляді та вимагати багатофакторну автентифікацію для отримання доступу.
- Поки ви їх захистите, ви можете записати паролі. Не пишіть їх на наліпках або картках біля тієї, яку захищає пароль, навіть якщо ви вважаєте, що вони добре приховані.
- Увімкніть багатофакторну автентифікацію за наявності. Для входу до облікового запису багатофакількома типами облікових даних, наприклад для введення пароля та одноразового коду, створеного програмою. Це додає ще один рівень безпеки на випадок, якщо хтось вгадає або викраде пароль.

Злочинці можуть спробувати зламати пароль, але іноді простіше скористатися слабкостями людини і виманити його в неї. Якщо ви отримали повідомлення електронної пошти від інтернет-магазину (наприклад, eBay або Amazon) або телефонний виклик від «банку», який намагатиметься переконати вас про «законне» отримання пароля або іншої важливої інформації, це може бути фішингове повідомлення.

Карпенко Анна Миколаївна
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

РОЛЬ СУЧАСНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ІНФОРМАЦІЇ

В сучасному світі, де цифрові технології проникають у всі сфери життя, питання безпеки інформації стає все більш актуальним. З кожним днем зростає кількість кіберзлочинів, загрози кібератак та порушень приватності.

Таким чином, важливість сучасних технологій захисту інформації набуває все більшої ваги, оскільки вони стають вирішальними для збереження конфіденційності, цілісності та доступності даних у цифровому середовищі.

Незважаючи на те, що проблеми сучасних технологій кібербезпеки були предметом наукових дискусій у роботах Савченко В.С., Колосовський Є.Ю., Круць Е.М., Бандурко О.М., Березовська І.Р., Гнатюк О.С., Дзьобань О.П. та інших, насьогодні, зазначене питання не втрачає своєї актуальності.

У сучасних умовах глобалізації та зростаючої конкуренції, захист інформації стає надзвичайно важливим аспектом як для організацій, так і для державних підприємств та корпорацій України. Створення надійних систем захисту і збереження інформаційних ресурсів на рівні всієї організації і її окремих підрозділів стає все більш актуальним, а успішність таких заходів безпосередньо впливає на конкурентоспроможність організації в цілому.

У юридичній літературі, захист інформації - це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації та осіб, які користуються інформацією [1].

Одним із основних методів забезпечення безпеки інформації у складних інформаційних системах є удосконалення системного підходу до цієї проблеми. Під системним підходом мається на увазі не лише створення відповідних захисних механізмів, але й впровадження систематичного процесу, що застосовується на всіх етапах життєвого циклу інформаційної системи та використовує усі доступні засоби захисту.

Задорожнюк Н.О. вважає, що забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації під час війни [2, с. 106].

Зазначене свідчить, що захист інформації повинен бути розглянутий як невід’ємна частина всієї інформаційної системи, а не просто як окремий компонент.

Крім цього, багато проблем, пов’язаних із захистом цієї інформації, можуть бути вирішені шляхом відомих правових та організаційних заходів. Проте з урахуванням прогресу інформаційних технологій, спостерігається зростаюча потреба в застосуванні технічних засобів та заходів для її захисту.

Наприклад, організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, знищення носіїв інформації, ідентифікації користувачів;

- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформацій-них ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

- навчання правилам інформаційної безпеки користувачів [3, с. 7].

Комплексний (системний) підхід до побудови будь-якої системи містить в собі:

- аналіз об'єкта впроваджуваної системи;

- оцінка загроз безпеки цього об'єкта; аналізуються ресурси, які будуть використовуватися під час розробки системи;

- оцінка економічної доцільності проєкту;

- аналіз самої системи, її характеристик, принципів функціонування та можливостей для підвищення ефективності;

- взаємодія всіх внутрішніх і зовнішніх факторів [4, с. 15].

Сучасний ринок програмних продуктів містить різні програми для забезпечення інформаційної безпеки. Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, криптографічний захист інформації, захист від комп'ютерних вірусів тощо. Такі програми можна поділити на системні та прикладні програми. Для ефективного захисту слід використовувати комплексний підхід, який враховує як зовнішні, так і внутрішні загрози. Важливо поєднувати програмні, технічні та організаційні засоби і заходи. Побудова єдиної концепції інформаційної безпеки дозволить забезпечити всебічний захист і оптимальну політику безпеки. Всебічний аналіз даних та інформаційного забезпечення допоможе виробити оптимальну стратегію захисту.

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 [5, с. 106].

Підводячи підсумок, можна зазначити, що кожен підхід та засіб захисту інформації впливають на безпеку та захист інформації, а також на діяльність підприємства чи організації по-різному. Важливо розуміти, що потенційні загрози від недосконалих систем захисту інформації можуть завдати шкоду діяльності підприємства. Тому належне управління інформацією на підприємстві повинно враховувати останні досягнення в галузі програмного, технічного та інших аспектів забезпечення інформаційної безпеки.

Список використаних джерел:

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. №80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.
2. Задорожнюк Н. О. Сучасні технології бізнес-аналітики. Економічна аналітика: сучасні реалії та прогностичні можливості : збірник матеріалів міжнар. наук.-прак. конф. (Київ, 19 квітня 2019 р.). Київ, 2019. С. 105–107.
3. Ляпін К. Е. Виклики та можливості сучасності: комплексна система захисту інформації. Збірник матеріалів VI міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології»: тези доповідей, 20-21 квітня 2023 р. Кропивницький: ЦНТУ, 2023. 96 с.
4. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. посіб. та ін. 63-тє вид. Вінниця: ВНТУ, 2018. 119 с.
5. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

Кедик Єлизавета Миколаївна
курсант 203 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

ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОМП'ЮТЕРНИХ СИСТЕМАХ

В інформаційному суспільстві спостерігається експонентне зростання інтенсивності процесів інформаційного обміну та обробки даних, що викликає необхідність використання потужних комп'ютерних систем. До таких систем пред'являють такі вимоги, як висока швидкодія, великий обсяг пам'яті, здатність обробляти велику кількість транзакцій одночасно, підвищена надійність.

Надійність, яка є однією з головних вимог до комп'ютерних систем, адже від рівня надійності системи залежить, наскільки відповідальні інформаційні процеси їй можна довірити. Оскільки абсолютна надійність комп'ютерних систем та результатів інформаційних процесів, які у них виконуються, не може бути забезпечена, задачею досліджень є визначення критичних областей, де такі помилки та збої в роботі не допустимі.

В сучасних умовах глобалізації інформаційна безпека виступає одним з найголовніших чинників забезпечення умов реалізації національних інтересів, спроможності держави долати кризові явища при зовнішній агресії [1, с. 23]. Своєчасні ефективні заходи щодо управління інформаційною безпекою з боку держави, як основного суб'єкта забезпечення інформаційної безпеки, здатні подолати загрози соціально-економічному та політичному життю країни.

Штучний інтелект представляє собою результат людської діяльності здатний до логічного мислення, управління своїми діями, обґрунтовування своїх рішень, які не може коректувати в разі зміни умов.

ШІ (англ. Artificial Intelligence, або AI) – це набір технологій та методів, що здатні аналізувати дані, робити прогнози і виконувати завдання, які зазвичай вимагають людського розуму, такі як розпізнавання образів, прийняття рішень та взаємодія і з людьми [2, с. 94]. Зазначене тлумачення визначає ШІ, як потужний інструмент, спроможний виконувати завдання, які раніше виконувалися виключно за допомогою людських можливостей [3, с. 352].

Сьогодні, поширене використання ШІ призводить до масової автоматизації робочих місць, що призводить до великих соціальних викликів, а саме втрати цінності людської праці.

Основні труднощі при впровадженні штучного інтелекту в комп'ютерні системи полягають у неможливості передбачити всі можливі реальні ситуації та програмувати поведінку машини адекватно до них, а також у недостатній надійності та програмних помилках. Вхідні дані, на основі яких навчається штучний інтелект, можуть бути неточними.

Крім того, вказані недоліки при використанні систем штучного інтелекту призвели до безлічі інцидентів, включаючи ті, що мають летальний характер. Аналіз повідомлень про помилки штучного інтелекту дозволив визначити критичні помилки, які відносяться до таких сфер, де застосування систем штучного інтелекту пов'язане з великим ризиком [4, с. 21]. Це такі галузі, як медицина, військові дії, транспорт, виробництво, де працюють люди та роботизовані системи, небезпечні виробництва, ядерна енергетика, соціальне управління, судові процеси і таке інше.

Дослідники стверджують, що штучний інтелект - це ніщо інше, як програма, яка ґрунтується на статистиці. Точність роботи таких програм не перевищує 95% [4, с. 125].

Отже, при такому рівні недоліків необхідно бути обережними щодо довіри до систем штучного інтелекту у сферах, де на кону стоять людські життя. Розробники комп'ютерних систем з штучним інтелектом мають обов'язок забезпечити вбудовування в алгоритми процесів, які запобігають можливість шкоди людині. Хоча алгоритми стають все більш адекватними у моделюванні реальних ситуацій, вони ніколи не будуть ідеальними або бездоганними. Питання про припустимий рівень помилок, вартість помилки та переваги заміни людей на штучний інтелект

завжди буде на порядку денному. У майбутньому людина все ще буде приймати критичні рішення, незважаючи на розумність систем штучного інтелекту.

На сьогоднішній день немає жодних законодавчих норм, що регулювали б саме використання штучного інтелекту. Штучний інтелект, використовуваний у критично важливих інфраструктурах і галузях, пов'язаних із здоров'ям та безпекою людей, вважається високоризиковим. В світі структури перебувають на переломному етапі через застосування більш сучасного обладнання та програмного забезпечення для інформаційної безпеки. Зарубіжні фахівці з інформаційної безпеки підкреслюють значний потенціал інформаційного та психологічного впливу в умовах стрімкого розвитку технологій штучного інтелекту. Штучний інтелект може бути важливим інструментом моніторингу загроз та захисту персональних та державних даних у світлі впровадження нових моделей та технологій.

Список використаної літератури:

1. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.

2. Карпенко Ю. В. Етичні принципи застосування штучного інтелекту в публічному управлінні / Ю. В. Карпенко // Вісник Національної академії державного управління при Президентові України. – 2019. – №4. – С. 93-97.

3. Яровий К. В. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. 618 с.

4. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

5. Радутний О. Е. Кримінальна відповідальність штучного інтелекту. Інформація і право. 2017. № 2 (21). С. 124–132.

Ковальов Данило Олексійович
слухач магістратури НАВС

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, капітан поліції

ФІШИНГ ЯК ЗАГРОЗА В МЕРЕЖІ ІНТЕРНЕТ

Фішінг – це форма кібершахрайства, яка полягає в шахрайському отриманні конфіденційної інформації, такої як паролі, номери кредитних карток, інформація про банківські рахунки тощо. Зловмисники, які займаються фішінгом, намагаються видати себе за довірене джерело, наприклад, банк, компанію або інший інтернет-сервіс, і надсилають листи або повідомлення, щоб підманити свої жертви та змусити їх розкрити свої особисті дані. Зловмисники зазвичай використовують різні методи для виведення своїх жертв з рівноваги:

1. Фішінгові листи електронної пошти: Зловмисники надсилають електронні листи, які виглядають як офіційні повідомлення від довірених компаній або установ. У цих листах можуть міститися посилання на фішінгові веб-сайти, які запитують особисту інформацію.
2. Фішінгові веб-сайти: Зловмисники створюють фішінгові веб-сайти, які імітують офіційні сторінки банків, онлайн-магазинів або інших сервісів.

Користувачі, що потрапляють на такі сайти, можуть ненавмисно розкрити свої особисті дані, довіряючи, що вони взаємодіють з офіційним ресурсом.

3. Соціальний фішінг: Зловмисники можуть використовувати інформацію з соціальних мереж для створення персоналізованих фішінгових атак. Вони можуть вивчати інформацію про своїх жертв, щоб створити реалістичні листи або повідомлення, які здатні переконати користувача надіслати свої особисті дані.

Способи захисту від фішінгу:

1. *Будьте обережні*: уникайте відкривати сумнівні електронні листи або клікати на посилання в них; перевіряйте адреси електронної пошти відправника та докладно аналізуйте будь-які надзвичайно підозрілі повідомлення.
2. *Перевіряйте веб-адреси*: перш ніж вводити свої особисті дані на веб-сайті, переконайтеся, що веб-адреса починається з "https://" і має сертифікат безпеки.
3. *Навчайтеся*: підтримуйте свої знання щодо фішінгових методів та тримайте себе в курсі останніх трендів у цій сфері.

Фішінг є серйозною загрозою для всіх користувачів Інтернету, але за допомогою обізнаності та обережності можно зменшити ризики стати жертвою.

Козлинець Вікторія Олегівна
курсант 210 навчальної групи ННІ № 1 НАВС, рядовий поліції

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ КРИМІНАЛЬНОГО АНАЛІЗУ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сьогоднішній день використання можливостей кримінального аналізу відіграє важливу роль в Національній поліції України, допомагаючи виявляти злочини, розгадувати злочинні ситуації та розробляти стратегії протидії злочинності. Кримінальні аналітики мають у своєму розпорядженні певні інформаційні ресурси, відомості з яких потрібно використовувати під час здійснення своєчасного, оперативного та достовірного аналізу діяльності організованих груп та злочинних організацій підрозділами Національної поліції України.

Кримінальний аналіз базується на аналізі доказів, зібраних у ході розслідування, включаючи використання даних, технологій та професійного досвіду [1].

Даний аналіз можна визначити як розумову діяльність працівників правоохоронних органів (аналітиків). Це включає перегляд, оцінку та інтерпретацію інформації щодо незаконної та злочинної діяльності окремих осіб і груп, отриманої в ході або в рамках слідчих дій. Він також використовується для встановлення важливих зв’язків між вищезазначеною інформацією для подальшого використання при визначенні тактичних і стратегічних напрямків боротьби та запобігання злочинності. Кримінальний аналіз дозволяє підрозділам Національної поліції України розвивати нові напрями досудового розслідування кримінальних справ, якісно планувати окремі слідчі розшукові заходи, аналізувати стан ефективності досудового розслідування, оперативно-розшукової та профілактичної діяльностей щодо протидії злочинності, обробляти великі обсяги інформації шляхом відстеження та кореляції фактів за допомогою спеціальних аналітичних методів, аналізувати складні та розгалужені структури взаємовідносин між суб’єктами кримінальних та слідчих справ, виявляти тенденції розвитку злочинності та подальшого її запобігання, виявляти ключових «гравців» у злочинному світі та злочинних організаціях.

Процес аналізу злочинності – це серія дій або кроків, які роблять найбільш точні та обґрунтовані висновки з наданої інформації. Інформація збирається, оцінюється та систематизується. Фаза аналізу процесу починається зі збору відповідних даних і організації їх у форматі, який полегшує визнання їх важливості, опис даних допомагає ідентифікувати відсутню інформацію та вжити подальших дій зі збору інформації для її отримання. Водночас це забезпечує основу для використання індуктивних міркувань для розробки однієї чи кількох гіпотез щодо ключових аспектів злочинної поведінки.

Мета аналізу багатовекторної інформації полягає в тому, щоб зробити висновки про характер і масштаби злочинної діяльності та встановити конкретних осіб і організації, причетних до неї. Висновки цілком достовірні при прийнятті рішень і виконанні дій [2, с. 96]. Підрозділ аналітики національної поліції орієнтований на проведення оперативного, тактичного та стратегічного аналізу.

Оперативна аналітика розбиває інформацію на найважливіші компоненти, виділяє та структурує її семантичне наповнення і робить цю інформацію легшою для розуміння, щоб оперативні працівники могли досягти подальших результатів [2, с. 125].

Метою тактичного аналізу є оцінка характеру злочину, визначення ризиків, тенденцій і моделей злочинності, встановлення подій, інцидентів або місць підозрюваного злочину. Ця форма аналізу має короткострокову та середньострокову перспективу. Використовується безпосередньо для успішного вирішення конкретних завдань [2, с. 170].

Аналіз злочинності на стратегічному рівні формує основу для стратегічного планування в певній сфері державної політики, а також допомагає правоохоронцям у вдосконаленні методів, прийомів і тактики поліції. Наявні дані та інформація аналізуються з точки зору кількості та якості [2, с. 201].

Проте, слід зазначити, що і законодавство України не ідеальне, тому при використанні кримінального аналізу можуть виникати деякі проблеми. Відповідно до статті 25 Закону України “Про Національну поліцію” поліція здійснює інформаційно-аналітичну діяльність в рамках якої також здійснює інформаційно-пошукову та інформаційно-аналітичну роботу [3]. На жаль, слід відмітити недосконаліть ст. 8 Закону України “Про оперативно-розшукову діяльність”, яка не надає права оперативним підрозділам проводити аналітичну розвідку для виконання завдань оперативно-розшукової діяльності [4]. Саме відсутність таких стандартів може спричинити проблеми при судовій оцінці результатів кримінальних проваджень.

Отже, враховуючи вищевикладене, проблеми, пов’язані з використанням результатів кримінального аналізу злочинності в кримінальному судочинстві полягають у відсутності вказівок органів поліції країни регламентує порядок проведення аналітичних кримінальних провадження, чинний Кримінально-процесуальний кодекс України не передбачає можливості надання слідчим

письмових доручень працівникам аналітичного підрозділу правоохоронних органів, недосконаліть Закону України «Про оперативно-розшукову діяльність» щодо права бойових частин проводити аналітичну розвідку, а також брак спеціалістів-«аналітиків» у національних підрозділах поліції [5]. Тому знання у галузі кримінального аналізу – його видів, форм, сфер, умов і можливостей застосування – мають бути широко пропаговані, боротьби зі злочинністю. Знаннями, компетентністю і кваліфікаціями у сфері аналітики у різній мірі, повинні володіти як кримінальні аналітики та їх керівництво на всіх рівнях управління, так і особи, які здійснюють розшукові, оперативні дії, проводять дізнання і слідство. У теперішній ситуації належне використання кримінального аналізу є необхідним обов'язком усіх інститутів з боротьби з незаконною діяльністю. Проте, залишається чимало проблемних моментів, які стосуються визначення та єдиного розуміння поняття й видів кримінального аналізу, нормативно-правового регулювання його використання в оперативно-розшуковій діяльності і відповідно в практичній діяльності оперативних підрозділів Національної поліції України, використання результатів кримінального аналізу.

Список використаних джерел:

1. Гнусов Ю. В., Калякін С. В. Кримінальний аналіз у роботі підрозділів Національної поліції України. Протидія кіберзагрозам та торгівлі людьми: зб. мат. міжнар. наук.-практ. конф. 26 лист. 2019, с. 61.

2. Федчак І. А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.

3. Про Національну поліцію [Текст]: Закон України від 02.07.2015 р. №580-VIII // ВВР. 2015. № 40-41. Ст. 379.

4. Про оперативно-розшукову діяльність [Текст]: Закон України від 18.02.1992 р. №2135-XII // ВВР. 1992. № 22. Ст. 303.

5. Школьніков В. І. Використання результатів кримінального аналізу в кримінальному процесі України. Міжвідомча науково-практична конференція «Актуальні проблеми досудового розслідування», присвячена Дню слідчого України, 2017, с. 33-35.

Кошельник Іванна Леонідівна
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

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

На сьогодні загрози, які надходять з кіберпростору, відбуваються дедалі активніше та зазіхають навіть на національну безпеку. Враховуючи залежність сучасного життя від інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, унаслідок щоденного функціонування майже всіх аспектів суспільного життя у кіберпросторі набуває актуальності розробка організаційних та правових заходів його захисту.

Відомі вітчизняні науковці, такі як М.О. Будаков, В.М. Бутузов, М.М. Галамба, Р.А. Калюжний, Н.В. Камінська, В.В. Коваленко, Я.Ю. Кондратьєв, Б.А. Кормич, Ю.Є. Максименко, А.І. Марущак і Г.В. Новицький, розглядали різні аспекти розвитку та формування інформаційних відносин, а також проблеми боротьби з кіберзлочинністю. Крім того, зважаючи на те, що значна частина кіберзлочинів знаходяться поза межами статистики, актуалізується проблема латентної кіберзлочинності в Україні.

Кіберзлочинність, яка вперше згадувалась у літературі на початку 1960-х років, визначається як порушення прав і інтересів у сфері автоматизованих систем обробки даних. Зазначене поняття охоплює всі види злочинів, що відбуваються у сфері інформаційних технологій та телекомунікацій. Кіберзлочинність включає в себе злочини, скоєні у кіберпросторі за допомогою комп'ютерних систем чи мереж, а також інших засобів доступу до цього простору [1].

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

На нашу думку, протидія кіберзлочинності полягає у спільних заходах державного і приватного секторів, удосконаленні міжнародних правових засобів та внутрішнього законодавства, а також в організації інституційного механізму протидії кіберзлочинам.

Своєю чергою, дослідники пропонують поділяти їх на два типи: нові злочини, зумовлені сучасними технологіями, та традиційні, вчинені через комп'ютери та Інтернет. Однак, другий тип злочинів не має чіткого визначення, і державна статистика щодо них відсутня.

Наприклад, О. Копатін і Є. Скулишин визначають кіберзлочини як злочини, пов'язані з використанням комп'ютерних систем та діяння в кіберпросторі. В. Болгов вважає, що кіберзлочини – це різні суспільно небезпечні дії, передбачені законом, які порушують право на захист від несанкціонованого розповсюдження та використання інформації, а також права на володіння та користування інформаційними технологіями [3, с. 127].

Поняття кіберзлочинності включає в себе кримінальні правопорушення, пов'язані з використанням комп'ютерів, систем та мереж електрозв'язку. Зазначене охоплює механізми підготовки, вчинення або приховування злочинних дій, які використовують електронно-обчислювальні машини та мережі (у сферах платіжних систем), обіг незаконної інформації через комп'ютерні системи, а також порушення господарських відносин і приватної власності за допомогою електронних мереж [4].

Враховуючи вищевикладене слід зауважити, що наразі не існує уніфікованих рекомендацій або інструкцій щодо класифікації кримінальних правопорушень у кіберпросторі як кіберзлочинів. Вчені та практики не мають загальної думки щодо цього, що ускладнює визначення кримінальних діянь у цій сфері. Без чіткого розуміння або переліку таких злочинів складно зібрати об'єктивні статистичні дані про кіберзлочини.

Список використаних джерел:

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

2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/term/39984.

3. Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. К.: Національна академія прокуратури України, 2015. 202 с.

4. Кримінальний кодекс України. URL: http://zakon3.rada.gov.ua/ laws/show/2341-14/page.

Красненко Вікторія Костянтинівна
курсант 201 навчальної групи ННІ № 3 НАВС, капрал поліції

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

СУЧАСНІ ВИКЛИКИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

У сучасних умовах зафіксовано зростання кількості кібератак, що стає наслідком триваючої кібервійни та збільшення загрози з боку російських хакерів. Тому забезпечення ефективного кіберзахисту стає одним із найактуальніших завдань, оскільки у багатьох сучасних організацій різних галузей діяльності всю інформацію все частіше зберігають у цифровій або електронній формі на окремих комп'ютерах чи інших пристроях для зберігання даних.

Незважаючи на те, що проблеми кібербезпеки в Україні в умовах воєнного стану були предметом наукових дискусій у роботах Корнейка О.В., Корчевського М.В., Кудінова В.А., Хахновського В.Г., Ярового К.В. та інших, насьогодні, зазначене питання не втрачає своєї актуальності.

Слід зазначити, що поняття інформаційної безпеки є ще одним методом визначення безпеки даних, який включає в себе конфіденційність, цілісність та доступність даних. Інформаційна безпека України є важливою складовою національної безпеки і забезпечує захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу, а також інших важливих інтересів людини, суспільства і держави. Вона включає в себе забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, а також доступ до достовірної та об'єктивної інформації [2, с. 106]. Крім того, існує ефективна система захисту та протидії нанесенню шкоди через поширення негативних інформаційних впливів, включаючи скоординоване поширення недостовірної інформації, деструктивну пропаганду та інші інформаційні операції, а також несанкціоноване розповсюдження, використання та порушення цілісності інформації з обмеженим доступом. Більшість сучасних бізнес-даних зберігаються в електронному вигляді на серверах, настільних комп'ютерах, ноутбуках або в мережі Інтернеті, в той час як десять років тому конфіденційна інформація зберігалася в архівах та кабінетах перед тим, як бути перенесеною в Інтернет.

Останнім часом велика увага дослідників приділяється кібербезпеці та її різноманітним аспектам. Проте, багато ще залишається невідомим у зв'язку зі швидкими темпами розвитку електронних технологій та суспільства загалом. Нові можливості інформаційного впливу на суспільство породжують нові загрози безпеці, що вимагають постійного оновлення та удосконалення систем захисту [2, с. 106].

Тому на нашу думку, концепція кібербезпеки потребує перегляду в контексті стрімких змін у світі інформації та домінуючих тенденцій розвитку глобального суспільства, яке все більше орієнтується на «інформаційні» виміри.

Водночас аналіз чинного законодавства вказує на те, що існує ряд недоліків щодо регулювання питання кібербезпеки (оборони), які потребують негайного формування пропозиції щодо шляхів вирішення існуючих проблем з урахуванням європейської інтеграції.

У цьому контексті слушної є думка Черниш Ю.О. та Мальцевої І.Р. про те, що дані зараз здебільшого зберігаються в електронному або цифровому форматі, тому найбільше уваги приділяється кібербезпеці. Так звані кібератаки від комп'ютерних вірусів і хакерства стали серйозною загрозою для комп'ютерних систем і мереж у всьому світі. Сучасні організації повинні надсерйозно сприймати ці загрози та інвестувати час і ресурси, необхідні для захисту своїх цифрових активів, в кібербезпеку, або ризикувати потенційно шкідливими системними зломами та збоями [3, с. 94].

У висновку слід підкреслити, що для вирішення проблематики інформаційної безпеки необхідна комплексна стратегія, яка охоплює різні аспекти цього питання. Зокрема, важливо здійснювати постійний моніторинг та аналіз загроз, впроваджувати сучасні технології захисту даних, підвищувати обізнаність персоналу з питань кібербезпеки, а також співпрацювати з іншими країнами та міжнародними організаціями для обміну досвідом та взаємної підтримки.

Крім цього, важливо також регулярно оновлювати законодавство та нормативно-правову базу у сфері інформаційної безпеки, щоб відповідати новим викликам та загрозам. Тільки через комплексний підхід та спільні зусилля різних сторін можна досягти успішного вирішення проблем інформаційної безпеки і забезпечити стабільний розвиток суспільства в умовах цифрової епохи.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/ show/2163-19#Text.

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

3. Черниш Ю. О., Мальцева І. Р, Штонда Р. М. Аналіз деяких кіберзагроз в умовах війни: Електронне фахове наукове видання. Кібербезпека: освіта, наука, техніка, 4 (16), 2023. С. 37-44.

Краснощок Віктор Миколайович
кандидат технічних наук, доцент, доцент кафедри прикладних інформаційних систем Київського національного університету ім. Тараса Шевченка

Шестак Ярослав Іванович
директор інформаційного обчислювального центру головного центру інформаційних технологій Державного торговельно-економічного університету

ЗАХИСТ ІНФОРМАЦІЇ В ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Будь яка інформаційна система взаємодіє з даними. Відповідно захист даних є одною з головних задач функціонування самої системи. Захист персональних даних – задача особливої важливості. Саме персональні дані найчастіше є метою зловмисників, які атакують інформаційні системи. Так близько 75% усіх випадків витоку конфіденційної інформації у світі у 2019 році становили персональні дані. Це більше, ніж роком раніше, коли персональні дані становили 70% усіх зареєстрованих витоків. Близько 48% витоків персональних даних у 2018 році були спричинені діями зовнішніх зловмисників, а 45% були здійснені звичайними співробітниками (навмисно чи випадково). При цьому близько 70% витоків персональних даних з вини співробітників є випадковими, тобто викликані різними помилками і недбалістю персоналу [1].

Розглянемо два варіанти захисту персональних даних в інформаційних системах.

Хешування паролів в базах даних. Процес хешування призводить до того, що на виході з вхідних даних отримується такий рядок, з якого вже неможливо відновити вхідний рядок.

Тому він добре підходить для захисту персональних даних. Функцій хешування завжди генерують вихідні дані однакової довжини, а будь-яка зміна на вході завжди повністю змінює вихідний код (мал 1).

name_user	pass_hach
v1	$2y$10$UHl1MWiM9KtrDaPLZFjjq..EDstc9LD7YM5pf21HljN...
v2	$2y$10$y/GkaPKDkTPqRzgJcunos.k52jcJOxo6LCxU2XNnFcT...
v3	$2y$10$kBN4DmFtQiMCDBtlJQ/IReiEMDWZZNzGZNgPAYC4T/h...
v5	$2y$10$8Jpm52xfO97lny3T7T/rPO1ZYBZ80GmzQjzLtawDknE...
v6	$2y$10$/ysnmpLRUTy9nekBTu8AUuvKSIUFws04liKEdptuKpK...
v8	$2y$10$g8zUfUGRBg861NwmMs5p9OgV/hqD9yTTkhuDSZFBu64...

Мал. 1. Приклади хеш-паролів з використанням функція password_hash()

В отриманих хешах:

$2y – алгоритм шифрування,

$10y – параметри алгоритму,

все інше – хеш пароля після додавання солі.

Однією з найбільш популярних функцій хешування є функція password_hash (), яка забезпечує найбезпечніше хешування паролів, повільне в обчисленнях, використовує внутрішню сіль і хешує ітеративно.

Вхідний пароль автоматично обробляється випадковою сіллю (додатковий рядок, який приєднується до первісного значення) і що при багаторазовому хешуванні одного і того ж пароля на виході завжди виходять різні хеші. Таким чином, зловмисник не зможе використати заздалегідь підготовлену хеш-таблицю і буде змушений зламувати паролі індивідуально.

Захист персональних даних на мобільних пристроях з операційною системою iOS. Операційна система iOS пропонує розробникам прикладних інформаційних систем такий перелік способів для зберігання застосунків та персональних даних користувача [2]:

- у вигляді файлів з кількома ступенями захисту;
- з використанням UserDefaults;
- з використанням Keychain;
- з використанням CoreData;
- з використанням СУБД SQLite;
- у вигляді файлів типу ключ-значення.

Keychain є найбільш безпечним способом збереження невеликих обсягів даних [3]. Такий рівень захищеності забезпечується, в першу чергу, апаратними особливостями реалізації цього підходу.

Справа в тому, що ця ділянка пам’яті вмонтована в основний процесор мобільного пристрою, що виключає можливість отримання доступу до пам’яті зі зміненим процесором.

Щоб мати можливість використовувати технологію Keychain, розробник спочатку має імпортувати системну бібліотеку Security. Keychain підтримує такий перелік операцій із елементами даних, що необхідно зберегти:

- додавання нових елементів даних;
- пошук елементів даних;
- оновлювання елементів даних;
- видаляння елементів даних.

Зберігання даних за допомогою Keychain, як і у випадку із записуванням до файлів, також має кілька рівнів доступу, що доступні розробнику:

- рівень захищеності «When passcode set». Такі елементи доступні, лише коли пристрій розблоковано. Для цього на пристрої має бути встановлено пароль. Якщо користувач видаляє пароль із пристрою, то усі елементи з цим рівнем захисту автоматично видаляються.
- рівень захищеності «When unlocked». Такі елементи доступні, лише коли пристрій розблоковано. Якщо на пристрої не встановлено пароль, то він завжди вважається розблокованим.
- рівень захищеності «After first unlock». Доступ до цих елементів неможливий, доки користувач не розблокує пристрій після перезавантаження; якщо на пристрої не встановлено пароль, то він завжди вважається розблокованим.

Інші способи зберігання даних на мобільних пристроях, що мають операційну систему iOS, не мають змоги безпечно зберігати дані. В Keychain варто зберігати:

- дані, які потребують найвищого рівня захисту (як-от, пароль від банківського застосунку);
- дані невеликих розмірів;
- дані, доступ до яких потрібно забезпечити з кількох потоків [4].

Вибір і використання правильного підходу для забезпечення надійного і безпечного зберігання цінних даних є на плечах розробника. Відповідно, інженери-програмісти, яким доручено забезпечити надійність збереження даних користувачів, мають бути обізнані про способи досягнення безпечного зберігання інформації, відповідно до операційної системи, для якої ведеться розробка.

Список використаних джерел:

1. Юридична газета online. Режим доступу: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/skandal-cifra-diya.

2. Data Persistence in iOS apps with Swift - Overview - Swift Tutorial. iOS App Templates. Режим доступу: https://iosapptemplates.com/blog/ios-development/data-persistence-ios-swift.

3. Keychain Services. Apple Developer Documentation. Режим доступу: https://developer.apple.com/documentation/security/keychain_services.

4. Інформаційний Інтернет-ресурс. Режим доступу: https://www.mysql.com.

Красько Ірина Андріївна
Здобувач ступеня вищої освіти НАВС

Науковий керівник:
Буренко Олег Володимирович
викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, підполковник поліції

ЗАГРОЗИ ВІД КІБЕРАТАК В УМОВАХ ВОЄННОГО СТАНУ

В умовах правового режиму воєнного стану кібератаки можуть відчутно вплинути на функціонування суспільства та стати загрозою національній безпеці.

Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі – відповідно до п. 5 ч.1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. Цей Закон визначає правові та організаційні основи забезпечення національних інтересів України у кіберпросторі, основні цілі державної політики у сфері кібербезпеки [1].

В умовах воєнного стану необхідно визначити форми та методи забезпечення інформаційної безпеки громадян з метою захисту суспільства не лише від деструктивного інформаційного впливу держав-агресорів та численних терористичних організацій, причетних до дестабілізації ситуації в нашій країні, а й від інших негативних інформаційних чинників, що дезорганізують національний інформаційний простір. Використання інформаційних технологій та механізмів для здійснення ворожих актів агресії проти громадян, незаконне використання інформаційних ресурсів інших країн, протиправна діяльність в інформаційному просторі, спрямована на дестабілізацію суспільства, використання інформаційної інфраструктури для поширення інформації, що розпалює міжетнічну та міжплемінну ворожнечу, ідей та теорій, що розпалюють ненависть, дискримінацію та насильство, використання інформації маніпулювання інформацією та багато інших загроз інформаційній безпеці створюють ризики [2, с. 23].

Основні загрози від кібератак в умовах воєнного стану:

1. *Втрати інформації*: кібератаки можуть призвести до викрадення або знищення конфіденційної інформації, наприклад, військових оперативних планів, даних про розробку зброї, даних державних установ та посадових осіб. Це може завдати шкоди національній безпеці та обороноздатності країни [3].

2. *Шантаж*: зловмисники можуть використовувати викрадену інформацію для шантажу державних установ, військових або цивільних осіб з метою отримання переваг або впливу на їхню поведінку.

3. *Пошкодження критичної інфраструктури*: кібератаки можуть спрямовуватися на критичну інфраструктуру, таку як енергетичні мережі, телекомунікаційні системи, системи водопостачання та інші. Пошкодження таких систем може призвести до серйозних наслідків для національної безпеки.

4. *Вплив на військові операції*: кібератаки можуть впливати на військові операції, зокрема на системи зв'язку, навігації та управління (атаки на системи зв'язку можуть зробити неможливим зв'язок між різними частинами армії, а атаки на системи навігації можуть спричинити неконтрольоване рухання техніки [4]).

Одна з найбільших кібератак на банківську сферу відбулася в липні 2017 року. Кіберзлочинці використовували шкідливий код під назвою «NotPetya», який поширювався через оновлення для бухгалтерського програмного забезпечення M.E. Doc, що використовується в Україні. Банки також використовували це програмне забезпечення і таким чином стали жертвами кібератаки. NotPetya використовував вразливість в операційній системі Windows, що дозволяло зловмисникам шифрувати комп'ютерні диски та вимагати від жертв викуп у біткоїнах. Крім того, вірус блокував доступ до систем банку, що призвело до значних фінансових втрат. В результаті цієї кібератаки кілька українських банків були змушені припинити роботу і призупинити обслуговування клієнтів.

Крім того, було пошкоджено низку комп'ютерів, що призвело до втрати даних та значних витрат на відновлення комп'ютерної інфраструктури.

Враховуючи вищевикладене слід зазначити, що Україна має необхідний потенціал для нарощування потенціалу у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам. Інструменти та технології кіберзахисту необхідно вдосконалювати, щоб зменшити ризик кібератак та забезпечити інформаційну безпеку. Тому необхідно вживати заходів для забезпечення високого рівня інформаційної безпеки та запобігання можливим кібератаки.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». – Вінниця: ХНУВС, 2023. – 176 с.

3. Інформаційно-аналітичний дайджест Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»: Кібербезпека в інформаційному суспільстві., №9 (вересень)

4. Інструменти інфомедійної безпеки в умовах воєнного стану URL:https://dspace.znu.edu.ua/jspui/bitstream/12345/12339/1/Vizniuk%202023.pdf.

Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС

ЗАЛЕЖНІСТЬ КРИПТОСТІЙКОСТІ ПАРОЛЮ КОРИСТУВАЧА ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ВІД КІЛЬКОСТІ МОЖЛИВИХ ДЛЯ ВИКОРИСТАННЯ СИМВОЛІВ

Для організації ефективного функціонування інформаційних систем спеціального призначення (далі – ІССП) необхідно забезпечити надійний авторизований доступ користувачів до інформаційних ресурсів, зокрема за допомогою парольного доступу. Державна служба спеціального зв'язку та захисту інформації України підготувала Рекомендації щодо підвищення рівня захищеності інформаційно-комунікаційних систем та інформаційних ресурсів державних органів і установ, в яких запропоновано державним органам і установам переглянути парольну політику з метою виявлення нестійких паролів, паролів, встановлених за замовчуванням або не встановлених взагалі [1].

Таким чином, створення стійких (надійних) паролів до злому є важливою складовою інформаційної безпеки ІССП. Станом на сьогодні існує низка робіт, що присвячені дослідженню окремих вимог щодо створення користувачами надійних паролів інформаційних систем взагалі [2-8], а також ІССП, зокрема МВС та Національної поліції України (далі – НПУ) [9-12].

Пароль – це набір символів, який користувач повинен ввести через обладнання вводу інформації, перш ніж він почне обробку інформації в інформаційній системі. Пароль призначений для підтвердження особистості або повноважень користувача і в інформаційних системах використовується для захисту інформації від несанкціонованого доступу. Головна перевага парольної аутентифікації – простота реалізації й використання. Проте, за сукупністю характеристик її слід визнати найслабшим засобом перевірки автентичності [13].

Як відомо, злом парольних систем може відбуватися за допомогою таких методів злому: 1) прямий перебір; 2) підбір по словнику; 3) метод соціальної інженерії; 4) перевірка по словнику найпопулярніших паролів; 5) перевірка послідовностей символів тощо [2]. Але необхідно відмітити, що при правильному використані паролі можуть забезпечити прийнятний для багатьох організацій, зокрема, МВС та НПУ, рівень безпеки [7].

Всі паролі умовно можна розділити на три види [11]: 1) легкі паролі; 2) паролі середньої складності, в яких присутні літери і цифри, але вони складаються з добре пізнаваних їх комбінацій; 3) стійкі паролі, які важко зламати шляхом логічного вгадування або методом перебору комп'ютерних програм.

Хакери використовують комп’ютери для перебору різних комбінацій літер, цифр і спеціальних символів. Сучасним комп’ютерам не складає труднощів за лічені секунди зламати короткі паролі, що складаються тільки з літер і цифр. Третина всіх паролів, що використовуються, зламаються шляхом простого перебору варіантів зі словника [5]. Департамент кіберполіції до Всесвітнього дня паролів, який відзначають в перший четвер травня, звернув увагу користувачів на важливість використання складних, багато символьних паролів для покращення захисту конфіденційних даних [6]. На підтвердження цього наводиться така статистика: хакеру для зламу паролю “123456” необхідно 1 секунда, паролю “283649Aa+” – 2 місяці, паролю “283649Aa+#-” – 9 років.

Найпростіші математичні обчислення дозволяють точно дізнатися про максимальну тривалість атаки (час, за який можна перебрати весь простір паролів заданої довжини, який буде залежати від технічних характеристик обладнання) (див. табл.).

Таблиця

Залежність криптостійкості паролю
від кількості можливих для використання символів

Довжина паролю в знаках	*Максимальний час перебору* (при швидкості 100 тис. варіантів за секунду)		
	36 символів (літери одного регістру та цифри)	*62 символи* (літери обох регістрів та цифри)	*95 символів* (усі друковані)
1	< 1 с	< 1 с	< 1 с
2	< 1 с	< 1 с	< 1 с
3	< 1 с	2 с	9 с
4	17 с	2,5 хв	13,6 хв
5	10 хв	2,5 год	21,5 год
6	6 год	6,5 днів	85 днів
7	9 днів	1,1 р.	22 р.
8	11 міс.	69 р.	2,1 тис. р.
9	32 р.	4,2 тис. р.	200 тис. р.
10	1 159 р.	266 тис. р.	1,9 млн р.
11	42 тис. р.	16,5 млн р.	1,8 млрд р.
12	1,5 млн р.	1 млрд р.	171 млрд р.

Примітки:

1. При розрахунку кількості можливих для використання символів було враховано, що абетка англійської мови складається з 26 літер та в одне поле можна також записати тільки одну цифру з 10 (0, 1, 2 …, 9).

2. В таблиці наведено округлені числа.

Формули прості: 1) кількість варіантів пароля = кількість можливих символів, з яких складається пароль, зводиться у ступінь кількості знаків, що складають довжину пароля; 2) максимальний час перебору = кількість варіантів пароля треба розділити на швидкість перебору для цього типу файлів.

На підставі даних, що наведені в таблиці, можна виявити такі закономірності: 1) криптостійкість паролю збільшується зі збільшенням кількості можливих для використання символів; 2) зазначене збільшення більш суттєво спостерігається при збільшенні довжини паролю; 3) довжина паролю, починаючи з 8 знаків і більше, забезпечує максимальну тривалість атаки, яка вже рахується роками, і може забезпечити прийнятний для багатьох організацій рівень безпеки.

Сьогодні російська федерація – країна-агресор, здійснює нічим не виправдану агресію проти України не тільки на нашій землі, а й у кіберпросторі. Використання кібератак – це повноцінна складова війни росії проти України. Українські інформаційні ресурси є важливою ціллю для російських військових [14].

Враховуючи вище зазначене, для забезпечення належного рівня інформаційної безпеки інформаційних систем спеціального призначення, зокрема МВС та НПУ, необхідно здійснити такі заходи: 1) розробникам програмного забезпечення цих систем передбачити можливість використання користувачами широкого діапазону символів; 2) користувачам цих систем обов'язково створювати стійкі паролі шляхом використання більше 8 знаків у паролі, а у якості символів – літери обох регістрів, цифри та спеціальні символи.

Список використаних джерел:

1. Рекомендації щодо підвищення рівня захищеності інформаційно-телекомунікаційних систем та інформаційних ресурсів державних органів і установ (ДССЗтаЗІУ. CERT-UA). ННЦІТ: [сайт]. URL: https://nncit.wunu.edu.ua/rekomendatsiyi-shhodo-pidvishhennya-rivnya-zahishhenosti/ (дата звернення: 15.04.2024).

2. Круглікова А. Д. Аналіз алгоритмів для оцінки стійкості паролів. Новітні інформаційні системи та технології. Полтава: ПНТУ, 2016. № 5. Режим доступу: http://journals.nupp.edu.ua/mist/article/view/589/511 (дата звернення: 15.04.2024).

3. Кудінов В. А. Загальний підхід щодо створення та використання надійних паролів користувачів інформаційних систем. Interdisciplinary research: scientific horizons and perspectives: I International Scientific and Theoretical Conference (Vol. 2), March 12, 2021. Vilnius, Republic of Lithuania: European Scientific Platform, 2021. PP. 47–48.

4. Кудінов В. А. Підвищення стійкості парольного захисту інформаційної системи до перебору шляхом використання даних рейтингових списків найбільш популярних в світі паролів. Сучасна спеціальна техніка. 2022. № 2. С. 67–76.

5. Buriachok V., Platonenko A., Semko O. Selection of the rational password generation method for the expected multiples. Ukrainian Scientific Journal of Information Security. 2019. Vol. 25. Issue 1. PP. 59–64.

6. Правила створення та використання надійних паролів – рекомендації кіберполіції. Кіберполіція України : [сайт]. URL: https://cyberpolice.gov.ua/article/pravyla-stvorennya-ta-vykorystannya-nadijnyx-paroliv--rekomendacziyi-kiberpolicziyi-3711/ (дата звернення: 15.04.2024).

7. Козачок В. А., Діхтяр М. В., Семко О. В. Особливості ідентифікації та авторизації в сучасних корпоративних інформаційно-телекомунікаційних системах. Сучасний захист інформації. 2017. № 2. С. 42–48.

8. Кохан О. В., Баришев Ю. В. Засіб генерування стійкого паролю. ВНТУ : [сайт]. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/download/9390/7674 (дата звернення: 15.04.2024).

9. Кудінов В. А. До проблеми щодо створення надійних паролів користувачів Інтегрованої інформаційно-пошукової системи МВС України. Актуальні проблеми управління інформаційною безпекою держави : матеріали VIII наук.-практ. конф. (Київ, 24 трав. 2017 р.). Київ: Нац. акад. СБ України, 2017. С. 54–56.

10. Кудінов В. А. Методика створення надійних паролів користувачів інформаційними ресурсами баз (банків) даних Національної поліції України. Міжнародна та національна безпека: теоретичні та прикладні аспекти: матеріали III міжнар. наук.-практ. конф. (Дніпро, 15 берез. 2019 р.). Дніпро: Дніпропетровський держ. ун-т внутр. справ, 2019. С. 261–263.

11. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). Сучасна спеціальна техніка. 2023. № 3. С. 42–49.

12. Кудінов В. А. Аналіз довжини стійкого паролю користувача інформаційних систем спеціального призначення Національної поліції України. Theoretical and Applied Cybersecurity (TACS-2023): зб. матеріалів I Всеукр. наук.-практ. конф., присвяченої 100-річному ювілею академіка В. М. Глушкова (Київ, 26 трав. 2023 р.). Київ: Нац. техн. ун-т України «КПІ ім. Ігоря Сікорського», 2023. С. 71–75.

13. Курятник О. В. Генератор паролів, що враховує механізми пам’яті людини. Інженерія програмного забезпечення: матеріали міжнар. наук.-практ. конф. Київ: Національний авіаційний ун-т, 2010. № 3. С. 74–78.

14. НКЦК: росія – країна-агресор у кіберпросторі. РНБО: [сайт]. URL: https://www.rnbo.gov.ua/ua/Diialnist/5463.html (дата звернення: 15.04.2024).

Лип'юк Анна Миколаївна
Курсант 202 навчальної групи ННІ № 3 НАВС, капрал поліції

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

ВИКОРИСТАННЯ МОЖЛИВОСТЕ СОЦІАЛЬНИХ МЕРЕЖ У ХОДІ РОЗСЛІДУВАННЯ ТА РОЗКРИТТЯ ЗЛОЧИНІВ

Використання соціальних мереж у сучасних реаліях стало не лише засобом комунікації, але й важливим інструментом для правоохоронних органів у розслідуванні та розкритті злочинів. Соціальні мережі, як засіб масової комунікації, створюють можливість отримання широкого кола інформації, яка може бути корисною у вирішенні кримінальних справ. Зокрема, вони можуть бути використані для отримання свідчень та доказів, виявлення свідків та потенційних підозрюваних, аналізу публічних висловлювань щодо подій, що мають правове значення, а також для встановлення контактів між учасниками правопорушення.

Зростаюча популярність соціальних мереж серед користувачів різних вікових груп і соціальних верств робить їх важливим інструментом для правоохоронних органів у вирішенні різних аспектів кримінальних справ. Однак, використання цього інструменту повинно відбуватися в рамках закону та з дотриманням прав людини і громадянина. Таким чином, використання соціальних мереж у розслідуванні та розкритті злочинів вимагає від правоохоронних органів професіоналізму, компетентності та дотримання принципів законності та об'єктивності.

Вивченням проблемних питань, пов`язаних із використанням можливостей соціальних мереж у боротьбі зі злочинністю, займалися вітчизняні та зарубіжні вчені, зокрема: В.В. Білоус, В.М. Бутузов, В.Б. Вєхов, А.Ф. Волобуєв, І.О. Воронов, В.Д. Гавловський, О.Ф. Гіда, С.В. Горова, А.М. Ішин, Д.М. Цехан, О.М. Юрченко та інші. Однак, наразі у сучасній юридичній науці відсутнє повноцінне та докладне дослідження, присвячене специфіці використання ресурсів соціальних мереж для виявлення та розкриття злочинів правоохоронними органами.

Використання можливостей соціальних мереж у ході розслідування та розкриття злочинів є корисним інструментом для правоохоронних органів. Проте це потребує ретельного та обережного підходу, оскільки інформація з соціальних мереж не завжди є надійною або може порушувати приватність осіб.

Соціальні мережі – це онлайн-платформи, які дозволяють користувачам спілкуватися, обмінюватися інформацією та взаємодіяти через віртуальні спільноти. Соціальні мережі часто використовуються для знайомств, спілкування з друзями та родиною, обміну новинами та інформацією (таким як текстові повідомлення, фотографії, відео) та споживати контент, а також для ведення бізнесу, маркетингу та реклами [1, с. 113].

У юридичній літературі, соціальні інтернет-мережі як об'єкт адміністративно-правового регулювання – це система прав фізичних і юридичних осіб (засновників, авторів аудіовізуального контенту та чисельних користувачів), які порушуються третіми особами в таких мережах, охорона яких здійснюється публічною адміністрацією на основі адміністративно-правових норм, у випадку неможливості їх захисту на основі цивільно-правових та інших соціальних норм [2, с. 48].

Своєю чергою, соціальні мережі можуть бути важливим інструментом для правоохоронних органів у розслідуванні та розкритті злочинів через наступні можливості:

- правоохоронні органи використовують соціальні мережі для збору інформації про підозрюваних, свідків або інші ключові факти, що стосуються справи, включати аналіз профілів користувачів, коментарів, фотографій або відео, що містять важливу інформацію;
- правоохоронні органи можуть реагувати на такі сигнали та проводити відповідні розслідування. Наприклад, аналіз друзів та контактів підозрюваних у соціальних мережах може допомогти встановити зв'язки між різними особами у справі, що допоможе в розслідуванні.
- правоохоронні органи використовують соціальні мережі для моніторингу діяльності різних груп та організацій, що можуть становити загрозу національній безпеці. Інформація з соціальних мереж може служити як доказ у кримінальних справах, якщо вона відповідає вимогам закону та може бути визнана судом [3, с. 23].

OSINT (від англ. Open Source Intelligence) – це збір, аналіз та інтерпретація відкритих джерел інформації з метою отримання розвідувальних даних. У соціальних мережах OSINT може бути корисним під час розслідування та розкриття злочинів в Україні, оскільки вони є важливим каналом комунікації для багатьох людей.

Наприклад деякі з основних OSINT інструментів, які можна використовувати для аналізу соціальних мереж у контексті розслідування злочинів в Україні, включають:

1. Пошукові системи: Google, Bing, Yahoo тощо. За допомогою цих систем можна знаходити публічно доступну інформацію про підозрюваних, потерпілих, свідків та інші ключові особи.

2. Спеціалізовані соціальні мережі: Наприклад, LinkedIn для пошуку професійної інформації, або Facebook, Twitter для вивчення публічних висловлювань осіб.

3. Аналітичні інструменти: Наприклад, соціальний аналізатор Sysomos або соціальний моніторинг Brandwatch дозволяють відслідковувати тематику та настрої груп людей у соціальних мережах.

4. Інструменти аналізу веб-сторінок: Наприклад, Wayback Machine для перегляду змін веб-сайтів у часі, або Google Cache для доступу до сторінок, які були видалені.

5. Інструменти для аналізу геоданих: Наприклад, Google Maps або OpenStreetMap для візуалізації місць подій та переміщення осіб.

6. Інструменти моніторингу соціальних мереж: Наприклад, Hootsuite або Sprout Social для відстеження та аналізу публічних дискусій.

Важливо пам’ятати про етичні аспекти використання OSINT, зокрема, збирання інформації лише з відкритих джерел та забезпечення конфіденційності осіб, чиї дані аналізуються [4, с. 123-124].

Додатково, важливо пам’ятати про важливість перевірки та підтвердження інформації, отриманої з відкритих джерел, перед тим як вона буде використана у розслідуванні. Зазначене допоможе уникнути поширення недостовірної або маніпулятивної інформації, яка може спотворити результати розслідування та завдати шкоди довірі громадськості до правоохоронних органів.

Крім того, у процесі використання OSINT-інструментів слід дотримуватися принципу прозорості та відкритості, сповіщаючи громадськість про хід розслідування та використання зібраної інформації у відповідності до вимог закону. Нарешті, успішне використання OSINT-інструментів у розслідуванні злочинів в Україні вимагає співпраці та координації між правоохоронними органами, громадськими організаціями та іншими зацікавленими сторонами. Тільки шляхом об’єднання зусиль можна досягти успішного результату в боротьбі з злочинністю та забезпечити правопорядок у країні [5, с. 78].

Використання OSINT-інструментів у соціальних мережах може бути дуже корисним у розслідуванні та розкритті злочинів в Україні, оскільки вони надають можливість отримати доступ до значної кількості відкритої інформації. Відповідно до законодавства та етичних стандартів, такий аналіз повинен бути проведений з урахуванням прав і свобод громадян, забезпечуючи конфіденційність та недопущення порушення закону. Важливо використовувати ці інструменти з урахуванням вимог законодавства та професійних етичних норм, уникати використання публічної інформації для незаконного або неетичного збирання особистих даних, а також забезпечувати об’єктивність та недискримінаційність у використанні отриманої інформації.

Крім того, важливо регулярно оновлювати та адаптувати інструменти для аналізу соціальних мереж у відповідь на зміни в соціальних та технологічних тенденціях, що дозволить підвищити ефективність розслідування та розкриття злочинів. Крім цього, важливо навчити персонал правильно використовувати соціальні мережі, уникаючи поширення недостовірної інформації та порушень конфіденційності. Залучення спеціалістів з інформаційної безпеки та права може допомогти забезпечити ефективне та законне використання соціальних мереж у розслідуванні злочинів.

Список використаних джерел:

1. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми (С. 142–146). Кримінальні загрози в секторі безпеки: практики ефективного реагування : матеріали панельної дискусії III Харків. міжнар. юридичного форуму «Право», м. Харків, 26 верес. 2019 р. / редкол.: В. Я. Тацій, Ю. Г. Барабаш, Б. М. Головкін, О. В. Таволжанський. Харків : Право, 2019. 176 с. URL: https://dspace.nlu.edu.ua/ bitstream/ 123456789/ 17042/ 1/ Shevchuk _142-146.pdf.

2. Грищук Р. В., Молодецька-Гринчук К. В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах. Сучасний захист інформації. 2018. № 1 (33). С. 43-52.

3. Гавловський В. Д. Правоохоронний моніторинг соціальних мереж. «Правова інформатика», 2014. № 3(43). С. 19–25.

4. Галунько А. В. Соціальні інтернет-мережі як об’єкт адміністративно-правового регулювання. Науковий вісник Ужгородського національного університету, 2013. С. 127-129.

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

Лукашенко Надія Дмитрівна
студентка 101_СМенеджмент навчальної групи ННІ № 1 НАВС

Науковий керівник
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС

НОРМАТИВНО-ПРАВОВІ ОСНОВИ ФУНКЦІОНУВАННЯ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МВС УКРАЇНИ

В Концепції розвитку електронного урядування в Україні, схваленої розпорядженням Кабінету Міністрів України (далі – КМУ) від 20 вересня 2017 року № 649-р, зазначено, що розвиток електронного урядування визначено одним з першочергових пріоритетів реформування системи державного управління [1]. Електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-комунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян. Тому серед основних напрямів державної інформаційної політики в Україні є: створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів [2]. Не залишається осторонь цих завдань і Міністерство внутрішніх справ (далі – МВС) України [3].

У Стратегії розвитку органів системи МВС на період до 2020 року, схваленої розпорядженням КМУ від 15 листопада 2017 р. № 1023-р, зазначено, що з метою ефективного реформування системи МВС в межах стратегічного пріоритету розвитку «Ефективне врядування, прозорість і підзвітність» передбачається зробити кроки щодо об’єднання і захисту відомчих інформаційних ресурсів органів системи МВС у межах єдиного інтегрованого інформаційного середовища, упровадження сучасного авторизованого доступу користувачів до інформаційних ресурсів органів системи МВС та надання їм доступу до відкритих даних органів системи МВС [4].

На підставі зазначеного в МВС України, з урахуванням Концепції програми інформатизації МВС на 2018-2020 роки [5], були вжиті заходи щодо створення єдиної інформаційної системи (далі – ЄІС) – інтегрованої інформаційної системи, що безпосередньо забезпечує реалізацію функцій її суб’єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв’язаних

функціональних підсистем, сервісів, програмно-інформаційних комплексів, програмно-технічних та технічних засобів електронної комунікації, які забезпечують логічне поєднання та інтеграцію електронних інформаційних ресурсів ЄІС МВС, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію шляхом використання функціональної підсистеми ЄІС МВС із спеціальними функціями [6].

Проблемні питання щодо створення ЄІС МВС розглянуті у роботах [7, 8]. Вирішенню проблеми нормативно-правового забезпечення функціонування інтегрованих інформаційно-пошукових систем (далі – ІПС) МВС України та Національної поліції України (далі – НПУ) присвячені праці [9, 10]. Питанням нормативно-правового закріплення прав людини щодо захисту і обробки персональних даних в ІПС МВС України та НПУ розглянуті у роботах [11, 12]. Рекомендаціям щодо основних шляхів створення належного рівня захищеності ЄІС МВС України присвячена праця [13].

Відповідно до Положення про ЄІС МВС України [6] законодавче забезпечення її функціонування складають Закони України «Про інформацію», «Про доступ до публічної інформації», «Про Національну програму інформатизації», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації», «Про електронні документи та електронний документообіг», «Про захист персональних даних», «Про електронні довірчі послуги», «Про публічні електронні реєстри», «Про основні засади забезпечення кібербезпеки України».

ЄІС МВС, згідно свого Положення [6], складається з: центральної підсистеми [14]; функціональних підсистем [15]; функціональних підсистем із спеціальними функціями; електронних інформаційних ресурсів суб'єктів ЄІС МВС; транспортної мережі передачі даних; центрів обробки даних, електронних комунікаційних мереж суб'єктів ЄІС МВС; комплексних систем захисту інформації підсистем ЄІС МВС з підтвердженою в установленому законодавством порядку відповідністю.

При цьому функціональними підсистемами ЄІС МВС є: 1) національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства; 2) інформаційний портал Національної поліції (далі – ІПНП) України [16]; 3) Єдиний державний реєстр транспортних засобів; 4) Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху; 5) система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі; 6) інтегрована міжвідомча інформаційно-комунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон; 7) інформаційно-комунікаційна система прикордонного контролю "Гарт-1"; 8) інформаційно-комунікаційна система 112; 9) Електронний реєстр геномної інформації людини; 10) Єдиний реєстр осіб, зниклих безвісти за особливих обставин; 11) Єдиний реєстр зброї;

12) Система управління силами та засобами цивільного захисту; 13) інші системи, реєстри та бази (банки) даних, створені суб'єктами ЄІС МВС в межах реалізації владних повноважень [6].

Необхідно відмітити, що мета обробки інформації у функціональних підсистемах ЄІС МВС установлюється нормативно-правовими актами, які регулюють діяльність відповідних суб'єктів ЄІС МВС, окремо для кожного визначеного електронного інформаційного ресурсу ЄІС МВС [6].

Розглянемо найбільш потужну функціональну підсистему ЄІС МВС інформаційно-комунікаційна систему «Інформаційний портал Національної поліції України» [16] – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності НПУ та її інформаційно-аналітичного забезпечення. Інформаційними ресурсами системи ІПНП є інформація, що використовується для наповнення та підтримки в актуальному стані: 1) 18 баз (банків) даних, які входять до ЄІС МВС та визначені ст. 26 Закону України «Про Національну поліцію» [17]; 2) баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень; 3) баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.

Законом України «Про Національну поліцію» регламентуються повноваження поліції у сфері інформаційно-аналітичного забезпечення (ст. 25), формування (ст. 26) та використання (ст. 27) поліцією інформаційних ресурсів, відповідальність поліції за протиправне використання інформаційних ресурсів (ст. 28) [17]. Відповідно до ч. 4 ст. 25 цього Закону діяльність поліції, пов'язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України «Про захист персональних даних», іншими законами України.

Таким чином, у роботі нами визначено нормативно-правові основи функціонування єдиної інформаційної системи МВС України, які містять відповідні закони та підзаконні нормативно-правові акти.

Список використаних джерел:

1. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 20 верес. 2017 р. № 649-р. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80 (дата звернення: 18.04.2024).

2. Про внесення змін до Закону України «Про інформацію» : Закон України від 13 січ. 2011 р. № 2938-VI. Відомості Верховної Ради України. 2011. № 32. Ст. 313. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2938-17#Text (дата звернення: 18.04.2024).

3. Про затвердження Положення про Міністерство внутрішніх справ України : Постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 878. Верховна Рада України : [сайт]. URL: https://zakon3.rada.gov.ua/laws/show/878-2015-%D0%BF (дата звернення: 18.04.2024).

4. Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : Розпорядження Кабінету Міністрів України від 15 листоп. 2017 р. № 1023-р. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80/conv (дата звернення: 18.04.2024).

5. Концепція програми інформатизації Міністерства внутрішніх справ на 2018-2020 роки, затверджена рішенням колегії МВС від 05 листоп. 2018 р. № 18км : Наказ МВС України від 11 груд. 2018 р. № 1004 (дата звернення: 18.04.2024).

6. Про затвердження Положення про Єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 1024. Урядовий кур'єр від 12 груд. 2018 р. № 235. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF (дата звернення: 18.04.2024).

7. Кудінов В. А. До питання щодо правонаступника інтегрованих інформаційно-пошукових систем органів внутрішніх справ України та організації їх інформаційної безпеки. Економічна та інформаційна безпека: проблеми та перспективи: матеріали Всеукр. наук.-практ. конф. (Дніпро, 14 квіт. 2017 р.). Дніпро: Дніпропетровський держ. ун-т внутр. справ, 2017. С. 94–97.

8. Кудінов В. А. Інновації в управлінні інтегрованою інформаційно-пошуковою системою Міністерства внутрішніх справ України. Інновації в управлінні соціально-економічним розвитком: матеріали І міжнар. наук.-практ. Інтернет-конф., присвячена 95-річчю Харківського національного університету міського господарства імені О.М. Бекетова (Харків, 05 берез. 2018 р.). Харків: Харківський нац. ун-т міського господарства імені О.М. Бекетова, 2018. С. 571–573.

9. Кудінов В. А. Проблеми нормативно-правового забезпечення функціонування інтегрованих інформаційно-пошукових систем Міністерства внутрішніх справ України та Національної поліції. Протидія злочинності: теорія та практика: матеріали VII Всеукр. наук.-практ. конф. (Київ, 19 жовт. 2016 р.). Київ: Нац. акад. прокуратури України, 2016. С. 330–332.

10. Кудінов В. А. Удосконалення правового регулювання функціонування інтегрованих інформаційно-пошукових систем Національної поліції України. Сучасна європейська поліцеїстика та можливості її використання в діяльності Національної поліції України: матеріали міжнар. наук.-практ. конф. (Харків, 11 квіт. 2019 р.). Харків: Харківський нац. ун-т внутр. справ, 2019. С. 152–154.

11. Кудінов В. А. Нормативно-правове закріплення прав людини щодо захисту і обробки персональних даних в інформаційно-пошукових системах Міністерства внутрішніх справ України та Національної поліції. Стан дотримання прав людини в умовах сучасності: теоретичні та практичні аспекти: матеріали VIII Всеукр. наук.-практ. конф. (Київ, 22 берез. 2018 р.). Київ: Нац. акад. внутр. справ, 2018. С. 184–188.

12. Кудінов В. А. Сучасний стан захисту прав і свобод людини, пов'язаних з обробкою інформації в інформаційних системах Міністерства внутрішніх справ України та Національної поліції. Захист прав людини: міжнародний та вітчизняний досвід: матеріали І міжнар. наук.-практ. конф. (Київ, 16 трав. 2019 р.). Київ: Нац. акад. прокуратури України, 2019. С. 315–319.

13. Кудінов В. А. Рекомендації щодо основних шляхів створення належного рівня захищеності Єдиної інформаційної системи МВС України. Кібербезпека в Україні: правові та організаційні питання: матеріали міжнар. наук.-практ. конф. (Одеса, 22 листоп. 2019 р.). Одеса: Одеський держ. ун-т внутр. справ, 2019. С. 58–60.

14. Про затвердження Порядку функціонування центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ України : Наказ МВС України від 16 верес. 2020 р. № 665. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z1092-20#Text (дата звернення: 18.04.2024).

15. Про затвердження Типового положення про функціональну підсистему єдиної інформаційної системи Міністерства внутрішніх справ України : Наказ МВС України від 29 квіт. 2021 р. № 324. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0609-21#Text (дата звернення: 18.04.2024).

16. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення: 18.04.2024).

17. Про Національну поліцію: Закон України від 02 лип. 2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40-41. ст. 379.

Малік Данило Андрійович
слухач магістратури НАВС

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, капітан поліції

ФІЗИЧНА БЕЗПЕКА

Фізична безпека комп'ютерних систем – це комплекс заходів, спрямованих на захист комп'ютерних систем, мобільних пристроїв, даних та програм від несанкціонованого доступу.

Фізична безпека комп'ютерних систем є важливою для захисту вашої особистої та ділової інформації. Вона може допомогти вам:

– Захистити ваші дані від крадіжки або втрати.

– Запобігти несанкціонованому доступу до вашого комп'ютера або мобільного пристрою.

– Захистити вашу особисту інформацію від розкриття.

– Зберегти цілісність ваших даних.

– Знизити ризик зараження вашого комп'ютера або мобільного пристрою вірусами.

1. Фізична безпека:

Контроль доступу:

– Встановіть замки на дверях та вікнах комп'ютерного приміщення.

– Використовуйте систему пропусків для контролю доступу до комп'ютерного приміщення.

– Встановіть камери спостереження для моніторингу комп'ютерного приміщення.

2. Захист обладнання:

– Зафіксуйте комп'ютери та монітори на столах.

– Використовуйте сейфи для зберігання носіїв інформації.

– Встановіть систему пожежогасіння в комп'ютерному приміщенні.

3. Безпека даних:

– Шифруйте дані на комп'ютерах та носіях інформації.

– Регулярно робіть резервні копії даних.

– Використовуйте програмні засоби для захисту даних (антивіруси, фаєрволи).

4. Інформаційна безпека:

Використання надійних паролів:

– Встановіть складні паролі для всіх облікових записів.

– Не використовуйте один і той же пароль для різних облікових записів.

– Регулярно змінюйте паролі.

– Оновлення програмного забезпечення:

– Встановлюйте останні оновлення операційної системи та програмного забезпечення.

– Використовуйте програмне забезпечення з відкритим кодом.

5. Навчання персоналу:

– Проведіть навчання персоналу з питань інформаційної безпеки.

– Слід ознайомити персонал з правилами та процедурами інформаційної безпеки.

– Навчіть персонал, як діяти у разі виникнення інциденту безпеки.

6. Регулярний перегляд:

– Регулярно переглядайте та оновлюйте план дій на випадок надзвичайних ситуацій.

– Регулярно проводьте аудит інформаційної безпеки.

– Регулярно оновлюйте програмне забезпечення для захисту даних.

Загальні рекомендації із дотримання фізичної безпеки комп’ютерних систем:

– Нагляд або блокування доступу до пристроїв.

– Блокування доступу для ОС Windows.

– Блокування доступу для MacOS.

– При введенні чутливих даних (паролі від облікових записів, банківські дані, персональна інформація тощо) слід прикривати другою рукою клавіші, що натискаються.

– Політика чистого столу – не залишати на столі носіїв з чутливими даними.

– Не використовувати невідомі або чужі комп’ютерні пристрої або носії даних.

Матвійчук Оксана Миколаївна
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

СУЧАСНИЙ СТАН КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Кожна соціально активна особа в Україні користується мобільними пристроями та інтернетом. Державні органи переходять на електронний документообіг. Стабільна діяльність банківського сектору, залізниць та авіатранспорту, а також великих підприємств залежить від стабільності кіберпростору. Україна переживає переломний етап, де війна перетворюється на битву не лише на полі бою, а й в інформаційному просторі. Внаслідок цього зростає кіберзлочинність, яка викликана як зовнішніми, так і внутрішніми загрозами, використовуючи перевантаженість правоохоронних органів та загальний хаос в суспільстві.

Хоча проблеми кіберзахисту в Україні вже досліджувалися у працях вчених, таких як Алпеєв А.С., Архіпов О.Є., Бакалинський О.О., Богданов О.М., Грибунін В.Г., Горбатько О.В., Мохор В.В., та Чепуренко Я.О., на сьогодні це питання стало найбільш поширеним та актуальним для суспільства, оскільки воно стосується всіх, хто працює з інформаційними технологіями.

У юридичній літературі кіберзлочин – це небезпечне діяння у кіберпросторі чи з використанням комп'ютерних технологій, передбачене законом, яке полягає в розкраданні або руйнуванні інформації в мережах і системах. У воєнний час це може спрямовуватися на дестабілізацію країни, крадіжку конфіденційних даних, а також на пошкодження державних інституцій і техніки [1].

Передумовами та чинниками, які формують загрози у сфері кібербезпеки України, є:

– недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі; – відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [2, с. 11].

Отже, в умовах воєнного стану в Україні, окрім існуючих правоохоронних органів, які борються з кіберзлочинністю, необхідно створити спеціальні підрозділи для захисту від кібервоєнних операцій супротивника та надавати адекватну відповідь на його інформаційну інфраструктуру.

Так, наприклад, правоохоронними органами України, США, Великої Британії, Японії, Філіппін, Індонезії, Малайзії було проведено такі операції: – «секс Торшн», внаслідок якої затримано 56 осіб, ліквідовано 4 транснаціональні кримінальні угрупування; – «Зевс», завданням якої було знешкодження міжнародної організованої злочинної групи, котра з метою викрадення фінансових реквізитів і доступу до банківських рахунків розповсюджувала шкідливе програмне забезпечення «Зевс». Під час операції знешкоджено інфраструктуру в мережі, що включала понад 40 тис. інфікованих комп’ютерів і серверів, левова частка яких знаходилась на території України. Спричинені збитки понад 300 млн доларів. Члени організованого злочинного угруповання – хакери з Одеси та Харкова на чолі з громадянином рф [3, с. 68].

Кібервійська, або служба кібероборони, повинна входити до складу Збройних сил України та містити структурні підрозділи, що здійснюють кіберрозвідку та спеціальні кібероперації, включаючи психологічні впливи на ресурси супротивника. Діяльність таких підрозділів повинна бути законодавчо регульована. Діяльність цих підрозділів повинна бути законодавчо регульована.

Це завдання складне через відсутність чітких норм щодо ведення військових дій у кіберпросторі, зокрема відносно їх початку, масштабів та розрізнення від традиційних кіберзлочинів. Проте поточна ситуація вимагає вирішення цього питання негайно.

Тому, у зв'язку з високим рівнем інформатизації суспільства, Україна повинна забезпечити ефективний механізм протидії кіберзлочинам, які є серйозною загрозою для національної безпеки. Оскільки ці злочини мають транснаціональний характер, правоохоронним органам України потрібне вдосконалене технічне забезпечення та компетентність для співпраці на міжнародному рівні у кримінальних розслідуваннях із цієї сфери, а також загалом у боротьбі з кіберзлочинністю. Україна має необхідні ресурси для розвитку своїх кібербезпекових здібностей для відповіді на сучасні виклики та загрози.

Список використаної літератури:

1. Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

2. Проєкт «Стратегія кібербезпеки України на 2021–2025 роки». Рада національної безпеки і оборони України: веб-сайт. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 15 квітня 2024 р.)

3. Демедюк С. В., Демедюк Т. С. Міжнародний досвід протидії кіберзлочинності. Вісник ХНУВС. 2014. № 4 (67). С. 65–75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/6023/Mizhnarodnyi%20dosvid%20protydii%20kiberzlochynnosti_%20 Demediuk%20SV_Demediuk_2014.pdf (дата звернення: 14 квітня 2024 р.).

Михайлюк Іванна Олександрівна
курсант 203 навчальної групи ННІ № 3 НАВС, капрал поліції

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

АНАЛІЗ ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ ПРАВООХОРОННИМИ ОРГАНАМИ

На сьогодні спостерігається досить значна інтеграція інформаційних технологій у діяльність правоохоронних органів. У цілому застосування штучного інтелекту, як напряму інформаційних технологій, в правоохоронній діяльності є доволі важливим та актуальним аспектом для України. Застосування методів і засобів штучного інтелекту при виявленні і розслідуванні злочинів у сфері інформаційних технологій є дуже актуальною темою в сучасному світі. Злочини в сфері ІТ стають все більш поширеними і складними, вимагаючи нових підходів та інструментів для їх виявлення та розслідування.

Дослідженню питань щодо впровадження технологій штучного інтелекту у виявленні і розслідуванні злочинів та проблем інформаційної безпеки присвячені чисельні роботи як вітчизняних, так і закордонних науковців, зокрема, О.В. Адамчука, О.А. Баранова, О.В. Глазова, Т.Г. Каткова, М.В. Карчевського, К.О. Хернес, С.Ю. Петряєва, О.Е. Радутного, Ю.М. Сидорчук, В.М. Фурашева, О.О. Ястреб, Є.О. Харитонова, О.І. Харитонова та інших. Проте, враховуючи думки зазначених авторів, доводиться констатувати, що в умовах постійного впливу зовнішніх та внутрішніх чинників необхідно приділити більше уваги дослідженню проблем штучного інтелекту в інформаційній безпеці як пріоритетній складовій національної безпеки України.

Термін штучний інтелект (далі – ШІ) є новим для українського законодавства і наразі відсутнє чітке визначення його правового регулювання. Впровадження інформаційних технологій, у тому числі технологій ШІ, є важливим елементом розвитку соціально-економічної, науково-технічної, оборонної, правової та інших видів діяльності у сферах, що мають загальнодержавне значення. Відсутність концептуальних засад державної політики у сфері ШІ унеможливлює створення та розвиток конкурентного середовища у зазначених сферах.

Технології ШІ дозволяють ефективно вирішувати різноманітні завдання у різних сферах життєдіяльності. Наприклад, ШІ широко використовують у сфері освіти, економіки, медичного обслуговування, охорони навколишнього середовища, державного управління та правозастосовної діяльності.

Слід зазначити, що існує різні погляди на тлумачення поняття ШІ. Визначення ШІ є багатогранним і використовується як наратив, за допомогою якого описуються інтелектуальні можливості комп'ютерів під час прийняття ними рішень [1, с. 16]. Тобто, це програма, яка обробляє дані та вирішує завдання, подібно до людського розуміння. Оскільки ШІ аналогічний комп'ютерним програмам, його можна регулювати, подібно до захисту літературних творів українським законодавством.

ШІ (англ. Artificial Intelligence, або AI) – це набір технологій та методів, що здатні аналізувати дані, робити прогнози і виконувати завдання, які зазвичай вимагають людського розуму, такі як розпізнавання образів, прийняття рішень та взаємодія і з людьми [2, с. 94]. Зазначене тлумачення визначає ШІ, як потужний інструмент, спроможний виконувати завдання, які раніше виконувалися виключно за допомогою людських можливостей [3, с. 352]. Сьогодні, поширене використання ШІ призводить до масової автоматизації робочих місць, що призводить до великих соціальних викликів, а саме втрати цінності людської праці.

О.Е. Радутний із цього приводу зазначає, що досягнення у розвитку штучного інтелекту можуть бути використані для вчинення злочинів, серед іншого в сфері інформаційних відносин, або сам він може становити безпосередню загрозу охоронюваним правам та законним інтересам людини, суспільства та держави [4, с. 129].

На думку Р.І. Благути та А.В. Мовчана, використання відеоінформації з камер відеоспостереження, встановлених на вулицях та в інших громадських місцях, є перспективним для розвитку оперативно-розшукової ідентифікації [5, с. 611]. Інтелектуальні системи безпеки, які використовують системи відеоспостереження на основі відеокамер зі ШІ, дозволяють попереджати злочини та терористичні атаки, внаслідок чого рівень злочинності в середньому може значно знижуватись [6, с. 83].

Загальні висновки цих дослідників можна підсумувати наступним чином:

1) внаслідок здатності до саморозвитку ШІ перетвориться на суперінтелект;

2) у суперінтелекта з'являться свої власні потреби і цілі (він може бути менш людяним, ніж розумний прибулець);

3) суперінтелект може спробувати використати людей проти їх волі (наприклад, з метою отримання доступу до ресурсів);

4) суперінтелект може забажати залишитися єдиним інтелектом навкруги;

5) людина як система зручно згрупованих атомів, може зацікавити суперінтелект як ресурс;

6) людство не є готовим до зустрічі із суперінтелектом і ще не буде готове багато років;

7) людство повинно навчитися тримати ШІ під достатнім контролем.

Отже, враховуючи вищевикладене, слід зробити наступні висновки, що аналіз проблематики використання технології штучного інтелекту правоохоронними органами залишаються поки що недостатньо дослідженими.

На нашу думку, важливо розглядати їх правовий статус у комплексі, враховуючи як недоліки, так і переваги. Необхідно ретельно вивчати та аналізувати ШІ, визначати їх місце та роль у майбутньому, прогнозувати можливі негативні наслідки та зменшувати їх вплив, а також виявляти проблемні аспекти, пов'язані з їх використанням у межах правового поля. Хоча ШІ мають великий потенціал для полегшення життя людини, важливо розуміти, що вони не можуть повністю замінити людину. Ефективність ШІ залежить від того, як і хто їх використовує та на які цілі. Зокрема, в майбутньому ШІ можуть стати причиною злочинності або навіть сприяти появі нових видів злочинності, що визначає необхідність подальших досліджень у цьому напрямку.

Список використаних джерел:

1. Сидорчук Ю. М. Філософсько-правові проблеми використання штучного інтелекту. Право і суспільство. 2017. № 3. Ч. 2. С. 16–19. URL: http://pravoisuspilstvo.org.ua/archive/2017/3_2017/part_2/6.pdf.

2. Карпенко Ю. В. Етичні принципи застосування штучного інтелекту в публічному управлінні / Ю. В. Карпенко // Вісник Національної академії державного управління при Президентові України. – 2019. – №4. – С. 93-97).

3. Яровий К. В. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. 618 с.

4. Радутний О. Е. Кримінальна відповідальність штучного інтелекту. Інформація і право. 2017. № 2 (21). С. 124–132.

5. Благута Р. І. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія / Благута Р. І., Мовчан А. В. - Львів: ЛьвДУВС, 2020. – 256 с.

6. Бугера О. І. Використання штучного інтелекту для запобігання злочинності. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 32 (71) № 6. 2021. С. 82–86.

Олексюк Роман Анатолійович
слухач магістратури НАВС

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, капітан поліції

ВІШИНГ: СУЧАСНА ЗАГРОЗА В МЕРЕЖІ ІНТЕРНЕТ

В сучасному цифровому світі інтернет-шахраї знаходять все більш винахідливі та складні способи обману. Однією з таких загроз є вішинг – вид інтернет-шахрайства, спрямований на отримання особистих даних та фінансових ресурсів користувачів. У цьому рефераті розглянемо основні аспекти вішингу, його наслідки та способи захисту від цієї загрози.

Вішинг – це форма інтернет-шахрайства, при якій шахраї використовують різні методи обману, щоб отримати доступ до особистих даних, банківських реквізитів та інших конфіденційних інформаційних ресурсів користувачів. Найчастіше вішинг відбувається через електронні листи, повідомлення в соціальних мережах, телефонні дзвінки тощо.

Типи вішингу:

- Фішинг – вішинг, який використовує електронні листи, які виглядають як листи від відомих компаній або установ, з метою викликати у користувача довіру та отримати від нього особисті дані.
- Веб-сайтовий вішинг – шахраї створюють фальшиві веб-сайти, що схожі на офіційні, для збору конфіденційних даних.
- СМС-вішинг – використання текстових повідомлень для введення користувача в оману та отримання від нього особистих даних.

Наслідки вішингу можуть бути дуже серйозними. Це може включати втрату фінансових коштів через шахрайство, втрату особистих даних, які можуть бути використані для ідентифікаційної крадіжки або шахрайства в мережі.

Способи захисту від вішингу:

- Ретельно перевіряйте джерела листів, повідомлень та веб-сайтів перед тим, як надавати будь-які особисті дані.
- Не відкривайте посилання або вкладення в сумнівних повідомленнях.
- Використовуйте надійне антивірусне програмне забезпечення та оновлюйте його регулярно.
- Ніколи не передавайте особисті дані через телефонні дзвінки або текстові повідомлення від невідомих джерел.

Вішинг є серйозною загрозою для користувачів інтернету, але з правильними заходами захисту можна уникнути попадання у пастку шахраїв. Освіта та свідоме використання інтернет-ресурсів є ключовими в боротьбі з цією формою кіберзлочинності.

Панченко Євгеній Вікторович
начальник 4-го управління Департаменту кіберполіції Національної поліції України, старший науковий співробітник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ

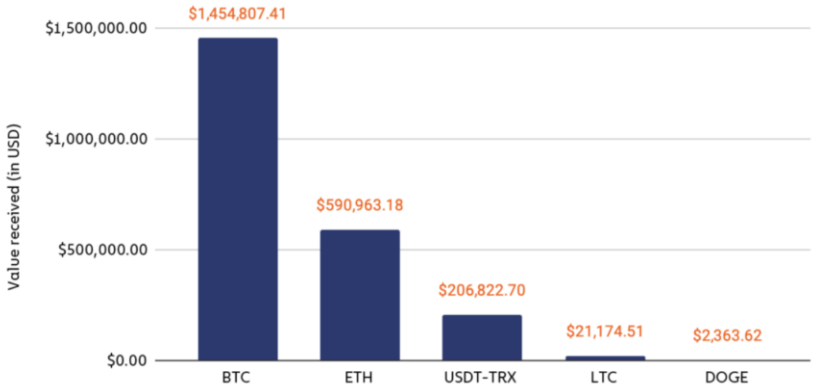
Овсянюк Дмитро Іванович
начальник аналітичного відділу (Центр кримінальної аналітики) Національної академії внутрішніх справ

АНАЛІЗ КЛАСТЕРІВ ТА АДРЕС ГАМАНЦІВ ВІРТУАЛЬНИХ АКТИВІВ (КРИПТОВАЛЮТИ) ДЛЯ ЗБОРУ КОШТІВ НА ДОПОМОГУ РОСІЙСЬКІЙ АРМІЇ ТА ІНШИМ НЗФ

Повномасштабна війна в Україні триває більше двох років, рішучі та результативні зусилля українських військових перегорнули сторінку історії, наповнивши її перемогами та звільнивши велику частину територій України (Київську, Чернігівську, Сумську, Миколаївську, Харківську області та частину Херсонської області), що в свою чергу зосередило епіцентр активних бойових дій на Донецьку, Луганську та частину окупованої Запорізької, Херсонської області та АРК Крим, де російські війська супроводжуючись різними незаконними збройними формуваннями, зокрема ПВК «Вагнер» і підбадьорюючись пропагандою російських дезінформаційних кампаній продовжують свою агресію проти України.

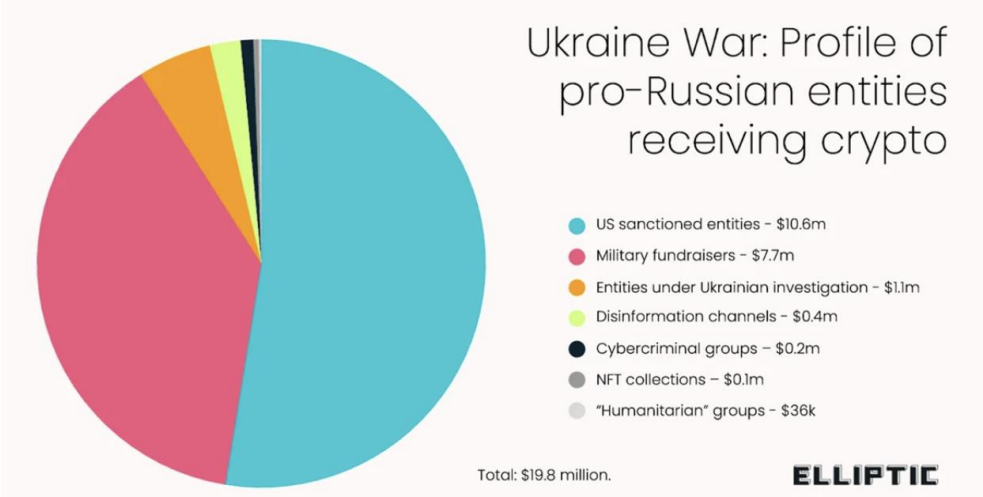
В той же час, з публікацій української розвідки та міжнародних партнерів стає зрозуміло, що існує велика кількість невирішених питань всередині російської армії, що супроводжується неякісним забезпеченням, зменшенням постачань, відсутністю системних підходів до організації зв’язку та навчання тощо. Ряд російських волонтерських груп та їхніх прихильників намагаються виправити ситуацію, в тому числі використовуючи соціальні мережі, зокрема Telegram та VK для збору коштів на військові закупівлі, розвиток БПЛА та радіозв’язку тощо, збираючи пожертви, у тому числі у віртуальних активах (криптовалюті) на закупівлю товарів та компонентів.

Як відомо, більшість криптовалют мають публічні блокчейни, що можуть бути використані для аналізу руху коштів, які надіслані чи відправлені з тієї чи іншої адреси [1]. За даними найвідомішої компанії з аналізу блокчейн «Chainalysis», з початку такими зборами займалися більше 54 організацій, які загалом отримали понад 2,2 мільйона доларів США у криптовалюті, переважно у вигляді Bitcoin та Ether. Також ними отримано значну кількість Tether, Litecoin та Dogecoin [2].



Статистичні дані щодо збору коштів на підтримку рф

Тим часом, представники компанії «Eliptic», що також має досвід у аналізі блокчейнів пишуть про 4,2 мільйона доларів, які зібрали росіяни на допомогу своїй армії та іншим незаконним збройним формуванням, що приймають участь у війні проти України. Ця цифра підрахована після накладення санкцій країнами членами НАТО, але до цього моменту цифра з неідентифікованих кластерів наближалася до 20 мільйонів доларів США, заявляють «Eliptic». Багато з цих платежів, ймовірно, є пожертвами, але деякі з них також можуть бути внутрішніми платежами залученим до зборів та створення дезінформації людям. Хоча ця цифра все ще може здатися невеликою порівняно зі зборами, які здійснюються Україною, трохи більше половини цих коштів пов'язані з суб'єктами, на яких поширюються санкції Сполучених Штатів Америки, що підкреслює постійні ризики для легальних сервісів віртуальних активів [5].



Статистичні дані щодо джерел збору коштів на підтримку рф

Серед тих, хто потрапив під санкції, є низка осіб, груп і неформальних мереж, які перейшли на криптовалюту з різних причин. Наприклад незаконне збройне формування ПВК «Вагнер», що отримало санкції від США, а також їх інформаційний канал підтримки «Оперативна група «Русич» – для них криптовалюта є джерелом збору коштів на додаток до кампанії пожертвувань у фіатній валюті. Воєнізоване угруповання «Русич», пов'язане з ПВК «Вагнер», серед суб'єктів, що потрапили під санкції OFAC (OFAC – Управління по контролю за іноземними активами Міністерства фінансів США), зібрало сотні тисяч доларів пожертв у криптовалюті. Адреси для пожертвувань були поширені через численні акаунти в соціальних мережах.

Для інших криптовалюта використовується більше як заохочення [3]. Високопосадовці так званої «Донецької народної республіки», серед яких є колишні організатори криптовалютних фінансових пірамід та особи, що потрапили під санкції, стверджують, що оплачують криптовалютою інформацію про позиції українських військових.

Під час нашого дослідження встановлено, що криптовалютні пожертви, надіслані цим організаціям, використовувалися на різні потреби - від фінансування проросійських пропагандистських сайтів до закупівлі військових товарів, таких як дрони, зброя, бронежилети, засоби зв'язку та інші засоби забезпечення.

Акаунти, які підтримують незаконні збройні формування, а також російську армію, часто публікують фотографії придбаного обладнання та опис того, як будуть використані майбутні пожертви. Ось один з таких дописів (переклад з російської): нам залишилося зібрати всього 150 тисяч рублів на безпілотник, який зможе привозити «подарунки» на позиції наших українських «друзів». Сподіваємося, що нам вдасться зняти його на відео і порадувати вас цікавими кадрами [4]. Оскільки один рубль коштує менше ніж 0,011 долари США, компоненти, необхідні для побудови БПЛА обійшлися цій групі лише у 3 400 доларів США (це було загальною ціллю збору). Отже, хоча багато організацій, які здійснювали збори, досягли лише чотиризначної цифри за рахунок збору коштів у криптовалюті, ці кошти все одно можуть зробити значний внесок у підвищення ефективності цих формувань.

Шляхом аналізу кампаній зі збору коштів, ми виявили низку підсанкційних осіб, які сприяли збору пожертв у криптовалюті на підтримку війни Росії в Україні. Олександр Жучковський, громадянин Росії, внесений до списку OFAC, використовував соціальні мережі для збору пожертв на користь терористичного угруповання «Російський імперський рух». Жучковський також підтримував проект «Террікон», який збирає пожертви у криптовалюті для підтримки НЗФ на Донбасі. На своєму сайті Terricon прямо вказував, що використовує криптовалюту у зв'язку з введенням санкцій, і навіть пропонував кілька NFT для збору коштів. Однак зараз сайт вже не активний, його було заблоковано [6].

Аналіз криптовалютних гаманців Terricon відображає його незаконний характер. Організація отримала приблизно 11% своїх коштів опосередковано від міксерів і відправила понад 29% своїх коштів на Bitzlato – біржу зі штаб-квартирою в Москві, яка сприяла відмиванню криптовалют на суму близько 1 мільярда доларів з 2019 року.

На зображенні джерело та кінцевий кластер надісланих коштів на гаманці проекту Terricon

Ми також виявили інші підсанкційні акаунти, пов'язані з благодійними рахунками для збору коштів на військових рф. Дописи з проросійського військового блогу «Рыбарь», який в тому числі збирає координати розташування українських військових, публікує недостовірну інформацію про російський наступ, були поширені широким колом проросійських акаунтів у соціальних мережах, включно з «Союзом добровольців Донбасу», на який OFAC наклав санкції 28 червня 2022 року.

Кілька операторів акаунтів у соціальних мережах вказали, що пожертви, надіслані їм, будуть безпосередньо спрямовані на користь «Донецької народної міліції» та «Луганської народної міліції», які в свою чергу пов'язані з «Народним ополченням Донбасу» - організацією, на яку 19 грудня 2014 року накладено санкції OFAC.

Переходячи до безпосередньо джерел походження фінансування кластерів зі збору коштів на допомогу армії рф, хотілось би акцентувати увагу, на те від кого надходять кошти, враховуючи, що увесь цивілізований світ маркує та позначає ці кластери як незаконні, а ті хто надсилає кошти стає спонсором російського тероризму. Найвірогідніше, і це помітно з результатів аналізу, що більша частина коштів вже мають незаконний характер, зокрема не тільки підсанкційний, але й пов'язаний з діяльністю нарко-шопів, послугами та товарами в дарк-нет, вірусами-вимагачами тощо.

Серед типових кампаній зі збору коштів на підтримку росії «Русич», «Катя-Валя», «Записки Ветерана» отримали найбільшу частину коштів саме від Дарк-нет маркетів, санкційних організацій, незаконних криптобірж та афілійованих з росією хакерських угруповань, в тому числі, які використовують та поширюють віруси вимагачі. На зображенні видно, що умовно не пов'язані за сферою діяльності незаконні кластери переплітаються і мають зв'язок з кластерами для допомоги російським військовим. Це не викликає подиву, адже саме така допомога незаконним збройним формуванням може безперешкодно здійснюватися без ризику втратити кошти, адже легітимні операції зазвичай блокуються у разі сумнівності джерела походження коштів.

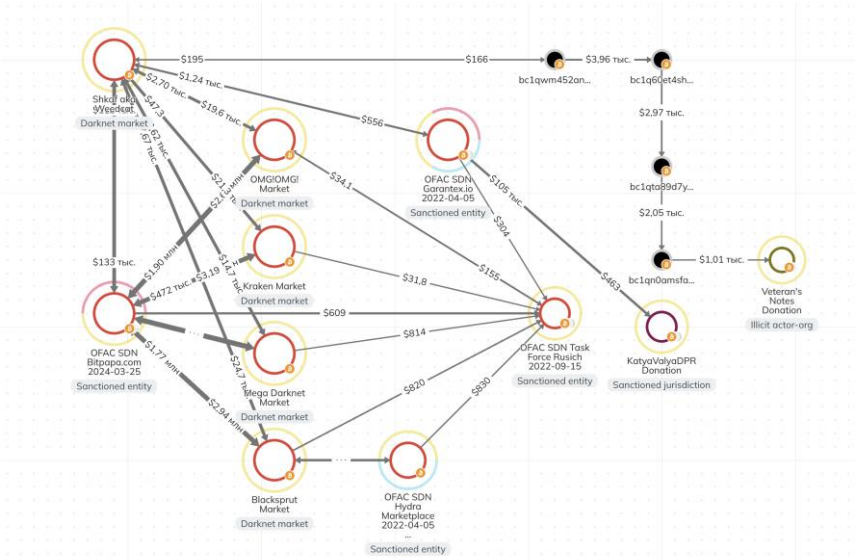


Схема руху коштів з незаконних кластерів, які фінансують терористичні угруповання та армію росії у війні проти України

Головною метою цього дослідження є бажання показати, що у повномасштабній війні, яка розпочата росією проти України, росіяни задіюють усі можливі джерела фінансування, у тому числі ті, що здійснюють негативний вплив на увесь світ (віруси вимагачі, дарк-нет маркетплейси, нарко-шопи), а отже і боротьба з НЗФ та особами, які збирають кошти з використанням віртуальних активів має бути комплексною, не лише на полі військових дій.

Усі наявні ресурси правоохоронних органів цивілізованого світу мають приділити увагу потокам коштів, які йдуть на фінансування росії та НЗФ, що приймають участь у війні проти України, адже рівень їх підтримки залежить на пряму від незаконних дій, що вчиняє злочинний елемент у середині країн Європейського союзу, Сполучених Штатів Америки та інших країнах. Усі ці факти можливо дослідити шляхом аналізу дарк-нет, а також подальшого руху коштів у криптовалюті.

Список використаних джерел:

1. Носов, В. В., Манжай, О. В. і Панченко, Є. В. (2022) «Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень», Право і безпека, 87(4), с. 108-124. doi: 10.32631/pb.2022.4.09.

2. Російські кампанії зі збору коштів у війні проти України [електронний ресурс] режим доступу: https://www.chainalysis.com/blog/pro-russian-crypto-donations-war-in-ukraine/

3. Прокремлівські неонацистські угрупування підбурюють до тортур та вбивств цивільного населення в Україні [електронний ресурс] режим доступу: https://www.theguardian.com/world/2022/oct/02/pro-kremlin-neo-nazi-militia-inciting-torture-murder-ukrainian-prisoners

4. Проект «Призма» та Олексій Муратов пов’язані особи з донецькими сепаратистами [електронний ресурс] режим доступу: https://behindmlm.com/companies/prizm-ponzi-and-aleksey-muratov-linked-to-donetsk-separatism/

5. Аналіз криптоплатежів на підтримку армії рф [електронний ресурс] режим доступу: https://www.elliptic.co/blog/analysis/crypto-payments-to-russian-military-fundraisers-reaches-20-million-amid-ukraine-counter-offensive-and-wagner-revolt

6. Веб-ресурс «Террікон» присвячений кампанії зі збору коштів на підтримку рф [електронний ресурс] режим доступу: https://web.archive.org/web/20220623213541/https://terricon.org.

Поворознік Артем В’ячеславович
аспірант Міжнародного гуманітарного університету

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Торгівля людьми, незважаючи на сучасний стан рівня розвиту суспільства та стан захищеності прав людини, залишається однією з найбільш актуальних проблем сучасності. Аналіз довоєнних статистичних даних Національної поліції України демонструє, що левову частку узагальнених статистичних даних цього злочину становить торгівля людьми з метою сексуальної експлуатації – 53%, з яких 59% становлять жінки, 27% хлопчиків і 14% чоловіків. Враховуючи ці дані, окремо варто відзначити високу латентність, яка становить 70% цієї кримінальної категорії [1, с. 26].

У цілому торгівля людьми має багатоаспектні прояви, включаючи сексуальне рабство, примусову працю, торгівлю органами та інші форми експлуатації. Порушена проблематика є глобальною масштабною проблемою, яка вимагає комплексного підходу та інноваційних стратегій для її подолання. У цьому контексті використання різного роду інформаційних технологій та технологій на основі штучного інтелекту набуває актуальності в боротьбі з торгівлею людьми. Інноваційні підходи та інтелектуальні рішення, що базуються на аналізі даних (у тому числі даних із відкритих джерел) та автоматизації аналітичних процесів, можуть сприяти виявленню, запобіганню та розслідуванню випадків торгівлі людьми, що дозволить забезпечити ефективнішу реакцію органів правопорядку та захист прав потерпілих.

Умови сьогодення, актуалізують проблематику застосування інформаційних технологій та штучного інтелекту у протидії торгівлі людьми. Сучасні технологічні рішення, які можуть бути застосовані для попередження злочинів у сфері торгівлі людьми, виявлення їх ознак та надання допомоги жертвам мають

великий потенціал в контексті їх практичної реалізації та загальної ефективності. Даний підхід надає можливості відкрити нові можливості для здійснення ефективних заходів протидії торгівлі людьми, що базуються на використанні інформаційних технологій та штучного інтелекту.

Перш за все, на нашу думку, актуальними є підходи у використанні інформаційних технологій та штучного інтелекту для вирішення завдань пов'язаних із аналізом великих обсягів даних за допомогою алгоритмів машинного навчання для виявлення відмінностей, закономірностей та маркерів, що характеризують злочини у сфері торгівлі людьми. Так, використання мультимодальних моделей в основі яких лежить машинне навчання, може стати ефективним інструментом вирішення проблематики торгівлі людьми.

Метою глибоких мультимодальних моделей є використання та створення моделей, здатних обробляти та співвідносити інформацію з різними модальностями [2]. Однак, ці моделі використовуються в медичних цілях, таких як ідентифікація ризику суїциду, посттравматичного стресового розладу та депресії [3, с. 59]. Однак ці моделі можуть бути використані в правоохоронній сфері, особливо в підрозділах кримінального аналізу [4, с. 86]. Використання таких методів та інструментарію дозволяє автоматично виділяти підозрілі маршрути, виявляти аномальні зміни у поведінці підозрілих осіб та ідентифікувати можливих злочинців.

Окрім наведеного вище, вбачається, що актуальним є створення спеціалізованих інформаційних систем та платформ для взаємодії та спільної роботи національних правоохоронних органів та громадських організацій у виявленні та реагуванні на випадки торгівлі людьми. Водночас зазначимо, що такі системи можуть мати транскордонний характер, тобто надавати можливість взаємодії правоохоронним органам різних країн. Такі системи можуть сприяти обміну даними, створюючи ефективні механізми виявлення та спільного вжиття заходів протидії злочинам у сфері торгівлі людьми, що може мати практичну цінність в тому числі у сфері кримінального аналізу.

Як відмічає Кисельов А.О., застосування кримінального аналізу здатне мінімізувати витрати часу працівників оперативних та слідчих підрозділів на вирішення поставлених завдань та підвищити якість їх інформаційно-пошукової діяльності [5, с. 65]. Крім того, в ході пошукової діяльності, передбачено використання різноманітного інструментарію такого як аналітичні програми, бази даних, інформаційні системи та інші [6, с. 100-101]. Використання інформаційних технологій та штучного інтелекту є позитивним в концепції збору інформації, адже, як зазначає Биков І.О., чим більший обсяг інформації, тим більше ймовірність встановити зв'язки з наявними даними та систематизувати їх [7, с. 40]. Таким чином, досить важливим є аспект використання інформаційних технологій та штучного інтелекту для збору та аналізу великих об'ємів даних та різного роду інформації стосовно злочинів торгівлі людьми.

Окрему увагу доцільно приділяти підтримці жертвам торгівлі людьми, так як інформаційні технології можуть стати інструментом підтримки даної категорії осіб, що бути реалізовано через створення систем їх комунікації або соціальної мережі чи інших онлайн-ресурсів для взаємної підтримки та психологічної допомоги або для звернення за допомогою та отримання конфіденційної підтримки та інформації.

Незважаючи на сучасний стан розвитку інформаційного суспільства та рівня організації боротьби із злочинами у сфері торгівлі людьми проблематика не втрачає своєї актуальності. Потенціал інформаційних технологій та штучного інтелекту для реагування на цю проблему є колосальним, а використання аналізу даних, машинного навчання та розробка спеціалізованих інформаційних систем можуть значно покращити ефективність виявлення, запобігання та розслідування випадків торгівлі людьми.

Водночас інформаційні технології можуть стати не лише інструментом для виявлення злочинців, але й сприяти підтримці та захисту прав потерпілих шляхом створення спеціалізованих онлайн-ресурсів та систем комунікації.

Позитивним у боротьбі зі злочинами у сфері торгівлі людьми може бути співробітництво між правоохоронними органами, громадськими організаціями та іт-компаніями, які можуть створити та інтегрувати ті чи інші іт рішення, програмні продукти та стратегії що зможуть призвести до значного зменшення випадків торгівлі людьми та забезпечити захист прав та гідності кожної людини.

Список використаних джерел:

1. Нєбітов А. А. Актуальні проблеми протидії оперативними підрозділами Національної поліції торгівлі людьми, вчиненої з метою сексуальної експлуатації. Використання досягнень сучасної науки й техніки в розкритті злочинів: матеріали міжвідом. наук.-практ. круглого столу, м. Київ, 25 лютого 2021 р. Київ: НАВС, 2021.С. 26-28.

2. Jabeen Summaira, Xi Li, Amin Muhammad Shoib, Songyuan Li, Jabbar Abdul. Recent Advances and Trends in Multimodal Deep Learning: A Review. Computer Vision and Pattern Recognition. 2021. URL: https://arxiv.org/pdf/2105.11087.pdf.

3. Stefan Scherer, Gale M Lucas, Jonathan Gratch, Albert Skip Rizzo, LouisPhilippe Morency. Self-reported symptoms of depression and ptsd are associated with reduced vowel space in screening interviews. IEEE Transactions on Affective Computing. 2016, Vol. 13. P. 59-73.

4. Ковалевський І. Сучасні можливості використання в кримінальному аналізу Deep multimodal models у межах протидії торгівлі людьми. Актуальні питання досудового розслідування: збірник матеріалів круглого столу (в авторській редакції), м. Кривий Ріг, 28 квітня 2023 року. Кривий Ріг: КННІ ДонДУВС, 2023. С. 85-87.

5. Кисельов А. О. Особливості здійснення кримінального аналізу на прикладі складання аналітичного звіту (за матеріалами УКА ГУНП в Дніпропетровській області). Бюлетень з обміну досвідом роботи №228/2021. РВВ ДНДІ. К., 2021, С. 63-67.

6. Биков І. Деякі адміністративно-правові аспекти впровадження ILP моделі в Україні. Імплементація ILP моделі в Україні: матеріали круглого столу, м. Одеса, 15 березня 2023 р. – Одеса : ОДУВС, 2023. – 133 с. С.100-103.

7. Биков І. OPEN DATA та OSINT в розслідуванні воєнних злочинів. Актуальні питання кримінального провадження у сучасних умовах: матеріали міжнародної науково-практичної конференції, м. Одеса, 31 травня 2023 р. - Одеса: ОДУВС, 2023. С.38-41. URL: https://dspace.oduvs.edu.ua/items/06a542fc-d533-45e0-a2ce-004339923324.

Прозоров Володимир Тотрадзович
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ, рядовий поліції

Науковий керівник:
Рог Вікторія Євгенівна
старший викладач кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ

МОЖЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ПРАВООХОРОННИМИ ОРГАНАМИ

Вступ. В сучасному світі штучний інтелект (ШІ) стрімко розвивається та впроваджується в різні сфери життя, й правоохоронна діяльність не є винятком. Завдяки своїм можливостям [1], ШІ може суттєво допомогти правоохоронним органам у боротьбі зі злочинністю, підвищити ефективність їх роботи та зробити її більш безпечною, використання штучного інтелекту може допомогти правоохоронним органам відстежувати злочинців та злочинні групи, визначати місцезнаходження злочинців, аналізувати відео- та аудіозаписи, шукати співвідношення між різними злочинами та правопорушниками тощо.

Виклад основного матеріалу. На наш погляд існує безліч способів, якими ШІ може бути використаний правоохоронними органами:

Прогнозування злочинів: ШІ може аналізувати великі масиви даних, такі як статистика злочинів, демографічні дані та дані про соціальні мережі, щоб виявляти закономірності та передбачати, де й коли з найбільшою ймовірністю можуть відбуватися злочини. Це дозволяє правоохоронним органам зосередити свої ресурси на запобіганні злочинам, а не на їх розслідуванні після скоєння.

Розслідування злочинів: ШІ може допомогти правоохоронним органам у розслідуванні злочинів, аналізуючи відео- та аудіозаписи, фотографії, дані з місця злочину та інші докази. ШІ може також допомогти їм виявляти зв'язки між різними злочинами та правопорушниками.

Ідентифікація злочинців: ШІ може використовуватися для ідентифікації злочинців за їхніми фотографіями, відбитками пальців, ДНК та іншими даними. Це може допомогти правоохоронним органам швидше розшукувати злочинців та притягувати їх до відповідальності.

Кібербезпека: ШІ може використовуватися для захисту комп'ютерних систем правоохоронних органів від кібератак. ШІ може також допомогти їм виявляти та розслідувати кіберзлочини.

Збір розвідданих: ШІ може використовуватися для збору розвідданих з відкритих джерел, таких як соціальні мережі, форуми та веб-сайти. Це може допомогти правоохоронним органам виявляти потенційні загрози та запобігати їм.

Розширене застосування ШІ правоохоронними органами яке може бути застосовано протягом найближчого часу:

1. *Кіберпатрулювання*: ШІ може використовуватися для моніторингу онлайн-активності, виявлення та запобігання кіберзлочинам, таким як торгівля наркотиками, дитяча порнографія та кібербулінг [2].
2. *Прогнозування тероризму*: ШІ може аналізувати дані соціальних мереж, публікації в блогах та інші онлайн-джерела, щоб виявляти потенційних терористів та запобігати терактам.
3. *Захист кордонів*: ШІ може використовуватися для автоматичного аналізу даних з камер спостереження, дронів та інших датчиків, щоб виявляти й затримувати нелегальних мігрантів та контрабандистів.
4. *Розслідування дорожньо-транспортних пригод*: ШІ може використовуватися для аналізу даних з камер спостереження, відеореєстраторів та GPS-пристроїв, щоб реконструювати події ДТП та визначати винуватців.
5. *Персоналізація правоохоронної діяльності*: ШІ може використовуватися для аналізу даних про злочинність та інформації про правопорушників, щоб розробляти персоналізовані стратегії запобігання злочинам та розслідування.
6. *Покращення взаємодії з громадою*: ШІ може використовуватися для створення чат-ботів та віртуальних помічників, які можуть відповідати на запитання громадян, надавати інформацію про послуги правоохоронних органів та приймати скарги.

7. *Підвищення прозорості та підзвітності*: ШІ може використовуватися для автоматичного збору та аналізу даних про роботу правоохоронних органів, щоб забезпечити прозорість та підзвітність їх дій.

8. *Навчання та підготовка*: ШІ може використовуватися для створення симуляційних середовищ та персоналізованих навчальних програм, щоб допомогти правоохоронцям розвивати свої навички та знання.

9. *Захист свідків та інформаторів*: ШІ може використовуватися для створення систем захисту свідків та інформаторів, які можуть забезпечити їхню анонімність та безпеку.

10. *Боротьба з корупцією:* ШІ може використовуватися для аналізу фінансових даних, виявлення корупційних схем та притягнення до відповідальності корумпованих чиновників [3].

Висновки. Використання технологій ШІ правоохоронними органами має багато потенційних переваг. ШІ може допомогти їм боротися зі злочинністю, підвищити ефективність роботи та зробити її більш безпечною. Однак важливо використовувати ШІ відповідально та етично, з урахуванням потенційних ризиків, таких як упередженість, дискримінація та зловживання владою.

Список використаних джерел:

1. Можливості використання штучного інтелекту у кримінальному провадженні в Україні | Вісник Харківського національного університету імені В.Н.Каразіна. Серія «Право». Наукова періодика Каразінського університету. URL: https://periodicals.karazin.ua/law/article/view/22344 (дата звернення: 17.04.2024).

2. KhNUIAIR: Репозитарій ХНУВС: Головна. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/26d850e6-49ce-4cc6-bf59-a0f14b6b4d40/content (дата звернення: 17.04.2024).

3. INTERPOL and UNICRI release blueprint for responsible use of AI by law enforcement. INTERPOL | The International Criminal Police Organization. URL: https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-and-UNICRI-release-blueprint-for-responsible-use-of-AI-by-law-enforcement (date of access: 17.04.2024).

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 сучаних 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 зазначенної 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 підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної 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 міждержавнаму рівні [5, с. 72].

Враховуючи вищевикладене слід зазначити, що сьогоднішні 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 волюнтаристськими 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 ефективної 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.

Термін «інформаційна війна» на сьогоднішній день має переважно публіцистичний характер і ще не отримав загального визнання. Зазначене підтверджується постійними обговореннями про те, що насправді означає цей термін, а також суперечками стосовно його коректності та практичного використання в контексті соціальних відносин, які часто характеризуються як інформаційне протистояння або конфлікт інтересів у сфері інформаційних систем [1, с. 58]. Таким чином, розробка та узгодження наукової термінології є окремою науковою проблемою.

Погоджуємось з думкою Ярового К.В., що протидія дезінформації безпосередньо залежать від якості інформаційної підтримки, оскільки основні зусилля практичних працівників із розслідування, розкриття та запобігати злочинам пов'язані з отриманням необхідної інформації [2, с. 76].

Дезінформація становить необхідну складову гібридних загроз, оскільки вона спрямована на ослаблення, дезорієнтацію, дестабілізацію та дезорганізацію політичних структур, функціонування державних і недержавних органів, їх безпеку, оборону, економіку, а також здатність реагувати на загрози та впливати на громадську думку та моральність населення в контексті гібридних воєн. Зв'язок між дезінформацією та іншими поняттями, такими як неправдиві новини, фейки та пропаганда, потребує додаткового розгляду [3, с. 185]. У публічній дискусії ці терміни часто сплутують або використовують як синоніми.

Фейк, як вид дезінформації, передбачає навмисне поширення неправдивої інформації з метою викликати позитивні емоції. Однак частіше він перетворюється на справжню дезінформацію, яка вводить в оману.

Тема поширення фейкових новин залишається актуальною та наочною. Сьогодні, у зв'язку з інформаційною війною з Росією, її актуальність стає безсумнівною, оскільки російські ЗМІ продовжують щодня створювати фейкові новини, спрямовані на дестабілізацію ситуації в нашій країні.

Враховуючи вищевикладене можна зробити наступні висновки, що соціальні мережі є однією з найбільш динамічно розвивающихся комунікаційних та інформаційних платформ. За кілька років вони пройшли значні зміни: від малих, розрізнених місцевих веб-сайтів до консолідованих компаній з глобальним охопленням і впливом. Соціальні мережі також стали частиною стрімкого розвитку мобільних технологій, які значно вплинули на поведінку людей, включаючи їх моделі використання соціальних мереж.

Згідно з цим, соціальні мережі виявилися надзвичайно потужним і ефективним інструментом для масового маніпулювання населенням. Їх широке використання сприяє поширенню дезінформації серед різних суб'єктів, як державних, так і недержавних. Тому важливо не лише продовжувати дослідження в цій галузі, але й поглиблювати їх ще більше.

Список використаних джерел:

1. Костюк І. А. Інформаційні війни в контексті революційних подій в Україні. Актуальні проблеми соціальних комунікацій : матеріали студентської наукової конференції, 22 травня 2014 р. Київ, 2014. С. 57-60.
2. Яровий К. В. Сучасні інформаційні технології в діяльності національної поліції України: матер. Всеукр. наук.-практ. семінару (м. Дніпро, 10 листопада 2022 р.). Дніпро: ДДУВС, 2022. 204 с.
3. Дубова Д. В. Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики? Київ: ТОВ «Видавництво Сталь», 2019. 254 с.

Сидорук Ольга 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

ДЕЯКІ АСПЕКТИ ВИКОРИСТАННЯ СУЧАСНОГО ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ В НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ

Останніми роками сучасні інформаційні технології інтенсивно впроваджуються майже в усі сфери державного життя України, в тому числі і в діяльність Національної поліції. Створені, впроваджені та успішно використовуються у боротьбі зі злочинністю міжвідомчі бази даних та інші комп’ютеризовані системи. Без використання сучасних телекомунікаційних технологій неможливо було б вирішити завдання підвищення ефективності та якості роботи державного поліцейського сектору. Охорона прав і свобод людини, захист інтересів суспільства і держави, боротьба зі злочинністю та інші завдання, які виконує поліція, вимагають постійного вдосконалення на основі сучасних досягнень науки і практики, розвитку, технологій і методів управління. У зазначеному контексті інформаційне забезпечення діяльності поліції відіграє важливу роль в успішному вирішенні правоохоронних завдань, оперативному реагуванні поліції на правопорушення, швидкому розкритті та розслідуванні злочинів.

На думку, Г.М. Шорохова під системою інформаційного забезпечення поліції розуміє сукупність взаємопов'язаних і взаємодіючих організаційних елементів та технічних засобів, що забезпечують розвідувальну підтримку Національної поліції України [1, с. 266]. За своїм змістом інформаційне забезпечення є поняттям системним, оскільки передбачає взаємну єдність певних елементів.

Інформаційні підсистеми, з іншого боку, є компонентами систем інформаційного забезпечення, призначеними для збору, накопичення, зберігання та обробки інформації з конкретних ділянок обліку, з акцентом на використання в більшості видів правоохоронної діяльності [2, с. 275]. Своєю чергою інформаційні підсистеми мають загальний характер і належать до галузевих інформаційних систем.

На законодавчому рівні роль поліції в рамках інформаційно-аналітичної забезпечення необхідне:

1) створення бази (банків) даних, що містяться в Єдиній інформаційній системі Міністерства внутрішніх справ України;

2) користування базою (банком) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) виконування завдань пов'язаним з пошуком та аналізом інформації;

4) здійснення обмін інформацією з іншими органами державної влади України, правоохоронними органами іноземних держав та міжнародними організаціями та інше [3].

Слід відмітити, що головним завданням підрозділів розвідки та аналізу, які функціонують у територіальних структурах Національної поліції, є забезпечення керівників на всіх рівнях достовірною інформацією щодо актуального стану оперативної обстановки та можливих тенденцій її розвитку. На основі цієї інформації вони розробляють конкретні заходи для запобігання злочинам та швидкого реагування на зміни в криміногенному середовищі. Крім того, вони об'єктивно оцінюють результати роботи поліції та оперативно-службової діяльності.

Натомість інформаційно-аналітичне забезпечення є ключовими не лише для ефективного управління органами поліції, але й для розробки та реалізації різноманітних програм запобігання злочинності, а також для майбутнього моделювання правоохоронної та правозастосовчої діяльності в конкретних соціально-економічних та демографічних умовах з урахуванням оперативної обстановки. Варто зазначити, що це допомагає управляти поліцією як складною правоохоронною системою в мінливому соціальному середовищі, оптимізувати саму систему та своєчасно розподіляти її ресурси [4, С. 209]. Тому, без інформаційно-технологічної підтримки управління зазначені досягнення були б неможливими.

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 [5, с. 106].

Таким чином, для вирішення завдань сучасного інформаційного забезпечення підрозділів поліції має бути запровадження єдиної політики інформаційного забезпечення, створення багатоцільової інформаційної підсистеми діяльності ОВС, удосконалення організаційного та кадрового забезпечення інформаційної сфери, інтеграція та систематизація інформаційних обліків на всіх рівнях ОВС, створення системи управління інформацією в ОВС, розбудови інформаційної мережі; створення умов для ефективного функціонування інформаційних обліків, забезпечення їх повноти, вірогідності, актуальності та безпеки; переоснащення інформаційних підрозділів сучасною потужною комп'ютерною технікою.

Список використаної літератури:

1. Шорохова Г. М. Інформаційне забезпечення діяльності територіальних органів поліції України // Електронне наукове фахове видання «Юридичний науковий електронний журнал». 2018. № 6. С. 264–267. URL: https://univd.edu.ua/science-issue/issue/3763.

2. Шорохова Г. М. Використання інформаційних технологій в діяльності Національної поліції України // VIII Міжнародна науково-практична конференція НАНР. Економіко-правові виклики 2017 року (14 січня 2017 року). Львів: НАНР-Національна академія наукового розвитку, 2017. Том 2. С. 274–278. URL: https://univd.edu.ua/science-issue/issue/379.

3. 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.

4. Управління органами Національної поліції України : підручник / за заг. ред. д-ра юрид. наук, доц. В. В. Сокуренка ; [О. М. Бандурка, О. І. Безпалова, О.В. Джафарова та ін. ; передм. В. В. Сокуренка] ; МВС України, Харків. нац. ун-т внутр. справ. Харків: Стильна типографія, 2017. 580 с.

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

Слободян Ольга Сергіївна
здобувач ступеня вищої освіти НАВС

Науковий керівник:
Буренко Олег Володимирович
викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, підполковник поліції

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

За оцінками світових експертів з кібербезпеки, у більшості країн світу спостерігається стійка тенденція до значного зростання кількості та масштабів кібератак, спрямованих на порушення конфіденційності, цілісності та доступності національних інформаційних ресурсів, особливо тих, що циркулюють на об'єктах критичної інформаційної інфраструктури.

Основними об'єктами кібератак є стратегічні інфраструктури країн (наприклад, ядерна, транспортна, хімічна та інші галузі промисловості; системи життєзабезпечення мегаполісів; фінансові, продовольчі та енергетичні державні системи; транспортні мережі; діяльність органів влади та правоохоронних органів). Атаки здійснюються через інформаційні та комунікаційні системи, особливо через автоматизовані системи управління. Ці системи є життєво важливими для повсякденного життя людей, економічної структури та функціонування державних установ [1, с.167].

Військова агресія Росії проти України та цифрова війна в кіберпросторі призвели до змін у глобальній моделі міжнародної безпеки. У цьому контексті все більше країн зацікавлені у зміцненні кібербезпеки та декларують стратегічні цілі у цій сфері. З початком війни Україна стала об'єктом численних кібератак, від яких постраждали державні установи, приватні організації та приватні особи. Компанії, що працюють у секторах критичної інфраструктури, таких як енергетика, телекомунікації, медіа та фінансові компанії, також повинні бути в стані підвищеної готовності, оскільки ці сектори часто визнаються пріоритетними цілями під час війни [2, с.267].

Також роботи додалося і в Кіберполіції яка на даний момент активно працює щодо роботи в напрямку перевірки осіб які причетні до коректування ворожих дронів та ракет на цивільну інфраструктуру. За 2023 рік було притягнуто до відповідальності більше 800 осіб по всій Україні.

З огляду на міжнародний контекст і постійне вдосконалення навичок російських кіберзлочинців і хакерів, на національному рівні слід приділяти належну увагу посиленню кібербезпеки та захисту даних.

Стійкість систем до зломів і атак важлива в кожному секторі. Цифрова безпека як новий тренд залишатиметься актуальною і в 2024 році [4]. Уряд роблять важливі кроки для зміцнення стану кібербезпеки як на нормативному, так і на методологічному рівні. Така системна робота допоможе вирішити проблему реагування на різні типи подій у кіберпросторі та значно посилить захист національних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури від кібератак. Забезпечення кібербезпеки України потребує посилення взаємодії та налагодження конструктивної і рівноправної співпраці між ключовими суб'єктами національної системи кібербезпеки України. Посилення кібербезпеки включає підготовку та реалізацію плану заходів з виконання Стратегії кібербезпеки до 2025 року, а також інкорпорацію та адаптацію законодавства ЄС до національних стандартів кібербезпеки [3, с. 269].

У чинному законодавстві не повною мірою імплементовані положення Конвенції Ради Європи про кіберзлочинність щодо обов'язкового зберігання та надання операторами, провайдерами телекомунікацій інформації, необхідної для розслідування кіберзлочинів [4, с.113], на запит правоохоронних органів; провайдери телекомунікаційних послуг не використовують механізми логування замість механізмів NAT (Network Address Translation), що ускладнює процес ідентифікації абонентів, а також залишається проблемою використання хакерських інструментів.

Список використаних джерел:

1. Тарасюк А. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights.* 2020. № 1. С. 167-172.

2. Горінов П. В., Драпушко Р. Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2023. № 1. С. 267-270.

3. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.23 р. № 299. URL: https://zakon. rada.gov.ua/laws/show/299-2023-п#Text

4. Гуржій С. В. Засади інституційно-функціонального забезпечення кібербезпеки в сучасних умовах. *Інформація і право.* № 2(37)/2021. С. 103-114.

Цимбал Єлизавета Андріївна
курсант 212 навчальної групи ННІ № 1 НАВС, рядовий поліції

Науковий керівник:
Буренко Олег Володимирович
викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, підполковник поліції

ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Ми живемо в епоху інформаційного суспільства, де інформаційні технології та телекомунікаційні системи проникають у всі сфери людського життя та державного управління. На сьогоднішній день жертвами хакерів можуть стати не тільки окремі особи, але й цілі держави. За наслідками та ефективністю використання кіберзброї, яку науковці все частіше порівнюють з зброєю масового знищення, кібербезпека стає однією з ключових проблем, яка викликає серйозне занепокоєння. І чим стрімкіше розвивається людство в інформаційних технологіях, тим більше зростає необхідність в захисті інформаційно-телекомунікаційних систем. Оскільки програмне забезпечення та автоматизовані системи стають дедалі більш вразливими до кібератак, тож не дивно, що уряди та суспільство активно працюють над пошуком найефективніших методів захисту особистих даних та Інтернет-ресурсів від цих загроз.

В Україні поняття «кібербезпека» вперше було використано у 2007 році [1], спочатку в контексті потреби «розробки та впровадження національних стандартів та технічних регламентів з використання інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, включно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність». З 2016 року під кібербезпекою в Україні розуміється стан захищеності життєво важливих інтересів людини, громадянина, суспільства та держави в кіберпросторі [2]. Згідно з Законом України [3], кібербезпека - це захищеність життєво важливих інтересів людини, громадянина, суспільства та держави під час використання кіберпростору, що забезпечує сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

В умовах воєнного стану захист суспільства від деструктивного інформаційного впливу з боку держави агресора та ряду терористичних організацій, які задіяні в процесі дестабілізації нашої країни, а також від інших негативних інформаційних факторів, які руйнують вітчизняний інформаційний простір, необхідно уточнити форми та методи забезпечення інформаційної безпеки громадян.

Стратегія кібербезпеки України [2] визначає пріоритетні заходи у забезпеченні кібербезпеки сектору безпеки й оборони, а саме:

– Створення і розвиток сил, засобів та інструментів для можливої відповіді на агресію у кіберпросторі, що може бути використана як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист).

– Проведення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони у кіберпросторі.

– Розвиток підрозділів кібербезпеки та кіберзахисту ЗСУ.

– Утворення єдиного підрозділу для забезпечення кібербезпеки та кіберзахисту ЗСУ на стратегічному, оперативному та тактичному рівнях.

– Розширення науково-виробничого потенціалу та системи підготовки спеціалістів з кібербезпеки для потреб органів сектору безпеки і оборони України.

Значна кількість загроз інформаційної безпеки створює наступні ризики:

– Можливість використання інформаційних технологій та механізмів для реалізації ворожих актів агресії проти громадян.

– Неправомірна діяльність в інформаційному просторі з метою дестабілізації суспільства.

– Незаконне використання інформаційних ресурсів інших держав.

– Маніпулювання інформацією з метою спотворення сталих моральних, етичних та культурних цінностей.

– Використання інформаційної інфраструктури для поширення ідей та теорій, що сприяють міжрасовій та міжнаціональній ворожнечі, а також пропаганди ненависті, дискримінації та насильства.

Глобальна кібербезпека мусить спрямовувати зусилля на захист та безпеку мережі з використанням наступних рівнів захисту інформації:

1) Попередження – доступ до бази даних та технологій надається лише авторизованому персоналу з відповідними спеціальними навичками;

2) Виявлення – забезпечення раннього виявлення злочинів та зловживань, навіть при наявності захисних механізмів;

3) Стримування – мінімізація збитків у разі вчинення правопорушень незалежно від заходів їх запобігання та виявлення;

4) Відновлення – забезпечення повного відновлення даних за наявності документованого та перевіреного плану відновлення [4].

Таким чином, для запобігання та вирішення проблем в галузі кібербезпеки, необхідно постійно проводити діагностування систем шляхом проведення спеціальних тестів, використання спеціалізованого обладнання та залучення кваліфікованих фахівців, які зможуть усунути причини можливих вразливостей. Також важливо пам'ятати, що ми всі знаходимося в одному великому мережевому просторі, тому навіть звичайний співробітник або військовослужбовець може стати жертвою будь-якого вірусу, що може призвести до зараження на всіх рівнях. Тому, одним із ключових аспектів кібербезпеки є проведення навчань з працівниками з метою запобігання та протидії кібератакам.

Список використаних джерел:

1. Стратегія національної безпеки України, затверджена Указом Президента України від 12.02.2007 No105/2007в редакції Указу Президента України від 8.06.2012 року No 389/2012. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/105/2007.

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 No 96.Офіційний вісник України. 2016. № 23.

3. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

4. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю.Є. Максименко, В. М. Желіховський. Київ: КНТ, 2020. 280 с.

Shaets E.O.
Cadet of the Faculty of Training Specialists for Criminal Police Units, Donetsk State University of Internal Affairs

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs

SOCIAL ENGINEERING AS A METHOD OF SHAPING PEOPLE'S CONSCIOUSNESS

Social engineering employs psychological manipulation techniques to shape behavior and beliefs, a tactic evident throughout history in various contexts like politics and marketing.

Central to social engineering is the capacity to influence consciousness, achieved through persuasion, coercion, deception, and manipulation. These methods impact beliefs, attitudes, values, and behaviors, molding consciousness itself. Political leaders might employ social engineering to sway public opinion or garner support for their policies, while advertisers may leverage it to sway consumer behavior by tapping into emotions or urgency. Similarly, cult leaders can use social engineering to foster dependence and loyalty among followers. Technology, notably social media, amplifies social engineering's reach, with platforms tailored to exploit human psychology through algorithmic content curation and the creation of echo chambers that reinforce existing beliefs and biases.

Social engineering techniques are frequently deployed online to coerce individuals into revealing confidential data or undertaking actions advantageous to the perpetrator. The internet serves as an optimal medium for social engineering due to its capacity to preserve anonymity and reach a broad audience. A prevalent online social engineering tactic is phishing, wherein perpetrators fabricate counterfeit websites or emails resembling authentic sources like banks or social media platforms. Subsequently, they deceive victims into disclosing login credentials or other confidential data, enabling access to the victim's accounts or identity theft.

Another technique of social engineering utilized on the internet is baiting, which entails creating a deceptive file or download masquerading as valuable or intriguing, such as a free software or movie download. Upon downloading, the victim unwittingly installs malware or other malicious software enabling the perpetrator to pilfer information or assume control of the victim's computer. Social media platforms are also frequent targets for social engineering endeavors. Perpetrators may fabricate fake profiles or disseminate false information or propaganda via social media. Furthermore, they may exploit social media to gather information about their targets, including their interests, connections, or whereabouts, to craft more convincing attacks.

To mitigate the risks of social engineering online, it is imperative to remain vigilant and skeptical of requests for information or actions. Always verify the legitimacy of websites or emails before divulging sensitive information, and exercise caution when downloading files or clicking on links. Keeping software updated and employing antivirus software can also safeguard against malware and other threats. Additionally, exercise discretion regarding information shared on social media and limit the personal information publicly accessible.

Awareness of the potential hazards of social engineering and maintaining vigilance against its manipulative tactics is crucial. This entails cultivating critical thinking skills, scrutinizing sources of information, and seeking diverse perspectives. By recognizing social engineering tactics, individuals can shield themselves from manipulation and make informed decisions aligned with their values and beliefs.

Шило Ігнат Єгорович
курсант 1 курсу факультету № 1 Донецького державного університету внутрішніх справ, рядовий поліції

Габорець Ольга Андріївна
доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ

СТРАТЕГІЇ БОРОТЬБИ З ДЕЗІНФОРМАЦІЄЮ У МЕРЕЖІ ІНТЕРНЕТ ПІД ЧАС ВОЄННОГО СТАНУ

У сучасному світі, який насичений технологіями та змінами, мережа Інтернет стала не лише основним джерелом інформації, але й ареною для боротьби за вплив та контроль над масовою свідомістю. У зв'язку з цим, проблема дезінформації, особливо у контексті воєнного стану, набуває нових вимірів та небезпек.

Воєнні конфлікти, незважаючи на свої прямі військові аспекти, часто відбиваються на сфері інформаційної війни, де використання дезінформації стає потужним інструментом. Умови воєнного стану створюють ідеальні умови для розповсюдження фейкових новин, маніпуляції громадською думкою та впливу на масову свідомість через Інтернет. Така дезінформація може мати серйозні наслідки, включаючи паніку серед населення, підірвання довіри до державних інституцій та навіть збройні конфлікти.

У юридичній літературі, захист інформації - це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації та осіб, які користуються інформацією [1].

Для того щоб ефективно боротися з дезінформацією у мережі Інтернет під час воєнного стану, потрібно розробити комплексні стратегії, які поєднують в собі технологічні, правові та освітні підходи. Ось деякі з можливих стратегій:

- моніторинг та аналіз інформації: важливо мати систему, яка постійно моніторить інформаційний простір, виявляє потенційну дезінформацію та аналізує її походження та поширення. Це може включати в себе використання алгоритмів штучного інтелекту для виявлення шаблонів та трендів у поширенні дезінформації;
- контрдезінформаційні кампанії: для протидії дезінформації потрібно активно впливати на інформаційний простір шляхом запуску контрдезінформаційних кампаній. Це може включати в себе публікацію фактів, розкриття маніпуляцій та викриття дезінформаторів;

- залучення громадськості та експертів може виявитися ключовим у боротьбі з дезінформацією. Для цього можна створити платформи, на яких громадяни зможуть виявляти та відстежувати поширення дезінформації. Також важливо співпрацювати з науковими установами та журналістами для аналізу та розкриття дезінформаційних кампаній.

Освітня робота: важливо проводити освітню роботу серед населення щодо виявлення та протидії дезінформації. Це може включати в себе навчання критичного мислення, навичок перевірки джерел та впізнавання маніпуляцій.

Співпраця з міжнародними партнерами: важливо співпрацювати з іншими країнами та міжнародними організаціями для обміну інформацією та координації зусиль у протидії дезінформації.

Ці стратегії, які поєднують технологічні та освітні підходи, можуть сприяти ефективній боротьбі з дезінформацією у мережі Інтернет під час воєнного стану. Однак їх успішне впровадження вимагатиме спільних зусиль з боку уряду, громадськості та міжнародних партнерів.

Список використаних джерел:

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. №80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

Шляхова Валерія Олександрівна
студентка 201_СПД навчальної групи ННІ № 3 НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ОСНОВНИХ ІНФОРМАЦІЙНИХ ПІДСИСТЕМ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ «ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ»

Від початку процесу інформатизації органів і підрозділів внутрішніх справ України минуло вже більше 50 років. За цей час накопичений чималий досвід використання різноманітних інформаційних та інформаційно-комунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення.

Серед них найбільш відома була Інтегрована інформаційно-пошукова система органів внутрішніх справ України («АРМОР»), функціонування якої відбувалось відповідно до її Положення, яке було затверджено відповідним наказом МВС України [1, 2].

Останніми роками в країні здійснюється реформа Міністерства внутрішніх справ України. Створено Національну поліцію України (далі – НПУ) як центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку. При цьому діяльність поліції спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України згідно із законом [3]. Для належного виконання цих завдань НПУ підтримує роботу низки інтегрованих інформаційно-пошукових систем. Проблемні питання, які виникають при цьому, розглянуто у статтях [4-7].

Станом на сьогодні серед цих систем найбільш потужною є інформаційно-комунікаційна система «Інформаційний портал Національної поліції України (далі – ІПНП)», Положення про яке затверджено наказом МВС України [8]. *ІПНП* – це сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності НПУ та її інформаційно-аналітичного забезпечення. Таким чином, ІПНП була створена з метою організації інформаційно-аналітичного забезпечення поліції. ІПНП містить у своєму складі десятки різноманітних інформаційних підсистем (далі – ІПС). Розглянемо правове забезпечення основних ІПС ІПНП, функціонування яких затверджено відповідними наказами МВС України.

1) *ІПС «Гарпун»* – створено з метою забезпечення оперативного реагування та прийняття ефективних управлінських рішень щодо розшуку транспортних засобів та номерних знаків [9].

2) *ІПС «Єдиний облік»* – створено з метою забезпечення формування інформаційних ресурсів поліцією під час реєстрації заяв і повідомлень про кримінальні правопорушення та інші події [10].

У п. 3 розділу І Інструкції [10] зазначено, що метою цієї системи є: 1) об’єднання інформації щодо заяв і повідомлень про кримінальні правопорушення та інші події від фізичних або юридичних осіб, що надійшли до органів поліції, в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп’ютерного та електронного комунікаційного обладнання; 2) забезпечення контролю за додержанням законності під час прийняття та реєстрації заяв і повідомлень про кримінальні правопорушення та інші події; 3) моніторинг стану оперативної обстановки в державі, виявлення районів зростання правопорушень для раціональної розстановки і маневрування силами та засобами органів поліції; 4) забезпечення інформаційно-аналітичної підтримки діяльності поліції, спрямованої на запобігання та розкриття правопорушень; 5) встановлення зв’язків між даними, що мають значення для

кримінального провадження та справ про адміністративні правопорушення; 6) формування статистичної звітності про результати роботи та дотримання законності органами (підрозділами) поліції під час реєстрації та розгляду заяв і повідомлень про кримінальні правопорушення та інші події.

Примітка: на наш погляд перераховані у п. 3 розділу І Інструкції [10] пункти краще назвати не метою цієї системи, а її завданнями. Це також стосується інших Інструкцій (Положень) до ІПС ІПНП, а саме: «Гарпун», «Атріум», «СЛІД», «Дорожньо-транспортна пригода», «Електронна розшукова справа», «Адміністративна практика», «Облік кривдника».

3) *ІПС «Атріум»* – створено з метою вжиття профілактичних заходів спостереження і контролю за поведінкою окремих осіб, щодо яких установлено адміністративний нагляд, а також контролю за прибуттям осіб, звільнених з місць позбавлення волі, до обраного ними місця проживання і поставленням на облік раніше судимих осіб [11].

4) *ІПС «СЛІД»* – створено з метою організації інформаційно-аналітичного забезпечення поліції [12].

5) *ІПС «Дорожньо-транспортна пригода»* – створено з метою забезпечення формування інформаційних ресурсів поліцією під час обліку дорожньо-транспортних пригод [13].

6) *ІПС «Custody Records»* – створено з метою покращення стандартів захисту прав затриманих осіб унаслідок запровадження електронної фіксації всіх дій щодо затриманої особи під час перебування під контролем поліції (фіксація, накопичення, зберігання) та пошуку інформації про затриманих осіб з моменту фактичного затримання [14].

7) *ІПС «Електронний кабінет ювенального поліцейського»* – створено з метою забезпечення формування поліцією інформаційних ресурсів під час обліку дітей, щодо яких поліцейські здійснюють профілактичну роботу [15].

8) *ІПС «Облік кривдника»* – створено з метою забезпечення формування поліцією інформаційних ресурсів під час обліку осіб, які вчинили домашнє насильство (кривдників) [16].

9) *ІПС «Адміністративна практика»* – створено з метою забезпечення формування інформаційних ресурсів поліцією щодо обліку адміністративних правопорушень, крім адміністративних правопорушень у сфері безпеки дорожнього руху, зафіксованих в автоматичному режимі, та порушень правил зупинки, стоянки, паркування транспортних засобів, у тому числі зафіксованих у режимі фотозйомки (відеозапису), та осіб, які їх учинили [17].

10) *ІПС «Розшук»* – створено з метою забезпечення формування інформаційних ресурсів поліцією під час здійснення оперативно-розшукової діяльності [18].

11) *ІПС «Електронна розшукова справа»* – створено з метою забезпечення формування інформаційних ресурсів поліцією під час здійснення оперативно-розшукової діяльності [19].

12) *ІПС «SOCTA»* – створено з метою забезпечення формування поліцією інформаційних ресурсів з обліку організованих груп та/або злочинних організацій, злочинних спільнот та сфер злочинної діяльності [20]. Відповідно до п. 4 розділу І метою створення ІПС «SOCTA» є автоматизація процесів збирання й узагальнення інформації та подальшого здійснення оцінювання загроз учинення тяжких та особливо тяжких злочинів організованими групами, злочинними організаціями, злочинними спільнотами [20].

Список використаних джерел:

1. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України : Наказ МВС України від 12 жовт. 2009 р. № 436. URL: https://zakon.rada.gov.ua/laws/show/z1256-09/conv#Text (дата звернення: 16.04.2024).

2. Про визнання таким, що втратив чинність, наказу Міністерства внутрішніх справ України від 12 жовтня 2009 року № 436 : Наказ МВС України від 06 січ. 2022 р. № 1. URL: https://zakon.rada.gov.ua/laws/show/z0089-22#Text (дата звернення: 16.04.2024).

3. Про Національну поліцію: Закон України від 02 лип. 2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.

4. Кудінов В. А. До питання щодо правонаступника інтегрованих інформаційно-пошукових систем органів внутрішніх справ України та організації їх інформаційної безпеки. Економічна та інформаційна безпека: проблеми та перспективи: матеріали Всеукр. наук.-практ. конф. (Дніпро, 14 квіт. 2017 р.). Дніпро: Дніпропетровський держ. ун-т внутр. справ, 2017. С. 94–97.

5. Кудінов В. А. Інновації в управлінні інтегрованою інформаційно-пошуковою системою Міністерства внутрішніх справ України. Інновації в управлінні соціально-економічним розвитком: матеріали І міжнар. наук.-практ. Інтернет-конф., присвячена 95-річчю Харківського національного університету міського господарства імені О.М. Бекетова (Харків, 05 берез. 2018 р.). Харків: Харківський нац. ун-т міського господарства імені О.М. Бекетова, 2018. С. 571–573.

6. Кудінов В. А. Проблеми нормативно-правового забезпечення функціонування інтегрованих інформаційно-пошукових систем Міністерства внутрішніх справ України та Національної поліції. Протидія злочинності: теорія та практика: матеріали VII Всеукр. наук.-практ. конф. (Київ, 19 жовт. 2016 р.). Київ: Нац. акад. прокуратури України, 2016. С. 330–332.

7. Кудінов В. А. Удосконалення правового регулювання функціонування інтегрованих інформаційно-пошукових систем Національної поліції України. Сучасна європейська поліцеїстика та можливості її використання в діяльності Національної поліції України: матеріали міжнар. наук.-практ. конф. (Харків, 11 квіт. 2019 р.). Харків: Харківський нац. ун-т внутр. справ, 2019. С. 152–154.

8. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення: 16.04.2024).

9. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 13 черв. 2018 р. № 497. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0787-18#Text (дата звернення: 16.04.2024).

10. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 14 черв. 2019 р. № 508. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0739-19#Text (дата звернення: 16.04.2024).

11. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Атріум» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 11 груд. 2019 р. № 1032. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0217-20#Text (дата звернення: 16.04.2024).

12. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 16 берез. 2020 р. № 257. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0319-20#Text (дата звернення: 16.04.2024).

13. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Дорожньо-транспортна пригода» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 15 лип. 2020 р. № 533. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0726-20#Text (дата звернення: 16.04.2024).

14. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Custody Records» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 24 трав. 2022 р. № 311. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0629-22#Text (дата звернення: 16.04.2024).

15. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Електронний кабінет ювенального поліцейського» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 27 груд. 2022 р. № 855. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0055-23#Text (дата звернення: 16.04.2024).

16. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Облік кривдника» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 16 січ. 2023 р. № 8. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0189-23#Text (дата звернення: 16.04.2024).

17. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Адміністративна практика» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 13 берез. 2023 р. № 180. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z0727-23#Text (дата звернення: 16.04.2024).

18. Про затвердження Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 28 черв. 2023 р. № 534. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z1486-23#Text (дата звернення: 16.04.2024).

19. Про затвердження Положення про інформаційну підсистему «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 05 лип. 2023 р. № 553. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z1504-23#Text (дата звернення: 16.04.2024).

20. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «SOCTA» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : Наказ МВС України від 08 листоп. 2023 р. № 902. Верховна Рада України: [сайт]. URL: https://zakon.rada.gov.ua/laws/show/z2041-23#Text (дата звернення: 16.04.2024).

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

МІЖНАРОДНИЙ ДОСВІД ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВОЄННОГО СТАНУ

У сучасному світі інформаційні технології стають невід'ємною частиною нашого повсякденного життя, які відіграють ключову роль у вирішенні складних завдань та оптимізують різноманітні процеси. Збільшення темпів інноваційних розробок спонукає до появи новітніх векторів вдосконалення у різних сферах життєдіяльності: медицині, промисловості, освіті, фінансах та правоохоронній діяльності.

Безумовно, вдосконалення правоохоронної системи та підвищення продуктивності протидії злочинності повинні здійснюватися за допомогою сучасних інформаційних технологій. Зокрема, штучний інтелект (надалі-ШІ) став звичайним явищем у діяльності правоохоронних органів, який широко використовується як інструмент протидії злочинності, відкриваючи перед нами нові сучасні можливості.

Теоретичні та практичні аспекти пов'язані з питаннями використання технологій ШІ були предметом чисельних досліджень. Проте, порушене питання потребує подальшого дослідження з метою розробки новітніх підходів та удосконалення нормативно-правової бази для ефективного використання технологій ШІ у ході розслідування та розкриття злочинів.

Багато досліджень, включаючи роботи Ezzeddine, Bayerl та Gibson [1, с. 863-864] дотримуються спільного напрямку використання поліцією можливостей ШІ цілей безпеки. Однак громадяни часто усвідомлюють і обережно ставляться до передових поліцейських можливостей, які можуть негативно вплинути на сприйняття легітимності поліцейських зусиль і поліції загалом. У цій роботі досліджуються суб'єктивні погляди громадян на використання ШІ поліцією, включаючи суперечності між безпекою, конфіденційністю та опором.

Elsherif [2, с. 347-349] стверджує, що протидія злочинності є необхідною та життєво важливою справою, яка оновлюється та розвивається відповідно до реальності свого суспільства, і водночас не опускається завіса юридичних теорій, які завжди приховували злочинця, іноді аналізуючи його. психологічно, іноді соціально, а іноді біологічно, щоб оцінити його кримінальну серйозність і застосувати відповідні заходи для запобігання його повернення до злочину. Знову ж таки, алгоритми, які є основою ШІ, виконують завдання точніше, швидше та дешевше. Однак новизна цього способу додала певної неоднозначності у визначенні його правової природи та законності.

Sachoulidou [3] приділяє увагу інструментам і технологіям, керованим ШІ, які використовуються на стадіях попереднього розслідування чи в рамках кримінального провадження, щоб декодувати людську поведінку та полегшити прийняття рішень щодо того, кого розслідувати, заарештовувати, переслідувати та, зрештою, покарати. Насамперед підкреслює існування постійної дилеми між метою підвищення оперативної ефективності поліції та судових органів та метою захисту основних прав постраждалих осіб. Крім того, наводяться аргументи на користь перегляду сфери захисту ключових фундаментальних прав, враховуючи, серед іншого, нові виміри, яких набула підозра.

Trifonov, Nakov та Mladenov [4] спрямовують дослідження на застосуванням інтелектуальних методів для підвищення безпеки в комп'ютерних мережах. Аналіз здійсненності різних методів ШІ показав, що метод, який однаково ефективний на всіх етапах кіберінтелекту, не може бути ідентифікований. У той час як для тактичної розвідки про кіберзагрози було вибрано та експериментовано багатоагентну систему, повторювані нейронні мережі пропонуються для потреб оперативної розвідки про кіберзагрози.

Tabi, Hewage, Bakhsh та Ukwandu [5, с. 104-105] досліджують підходи, натхненні ШІ, які використовує поліція для захисту дітей в Інтернеті. Розглянуті підходи є успішними в більшості ситуацій, але мають свої недоліки. Таким чином, усі зацікавлені сторони в сфері захисту дітей потребують такого розгляду. Крім цього, автори розглядають одностороннє використання ШІ для прогнозування та виявлення зловживань в Інтернеті на відміну від особистого розслідування та втручання.

Ismail, Muhammad, та Mosali [6, с. 161-162] представлено дослідження рейтингу 27 виявлених факторів, пов'язаних з інноваціями, які впливають напредставлено дослідження рейтингу 27 виявлених факторів, пов'язаних з інноваціями, які впливають на продуктивність ШІ в ОАЕ. Зазначені фактори були згруповані в чотири групи, а саме інновації процесу; управлінські можливості; особистий досвід та організаційна структура. Дослідження також виявило, що два фактори, якими є управлінські можливості та ШІ, сильно впливають на ефективність організації, тоді як інші три фактори, які обробляють інновації, особистий досвід і організаційну структуру, помірно впливають на ефективність організації в ОАЕ. Результати цього дослідження дозволять краще зрозуміти фактори, пов'язані з інноваціями, і те, як вони впливають на загальну продуктивність ШІ в ОАЕ.

Becker, S., Heuschkel M., Richter S. та Labudde D. [7, с. 176-177] дійшли спільного висновку, що під час судового переслідування основною метою є довести кримінальні правопорушення правильному винному, щоб засудити його на законну силу. Однак насправді цього може бути важко досягти. Зважаючи на місце скоєння злочину, можна припустити, що наявні достатні записи з камер відеоспостереження, які зафіксували злочинця на місці злочину.

Традиційні підходи та методи дослідження, такі як розпізнавання обличчя та аналіз ходи, швидко досягають своїх меж.

Gans-Combe C. [8] зосереджується на дослідженні використання ШІ у сфері права. Автор вважає, що робота слідчих і суддів може бути полегшена за допомогою цих інструментів, зокрема щодо пошуку доказів під час слідчого процесу або підготовки правових висновків, панорама поточного використання далеко не райдужна, оскільки вона часто суперечить реальність польового використання та викликає серйозні питання щодо прав людини. Однак зазначені елементи погано розуміються юридичним світом і можуть призвести до неправильного використання. Тому, виникає потреба визначити як користувачів штучного інтелекту в галузі права, так і способи його використання, а також потреба в прозорості, правила та контури якої ще належить встановити.

Розбіжності поглядів у тлумаченні визначення «штучний інтелект», відсутність належного правове регулювання у галузі кібербезпеки, а також недостатній рівень інформаційної освіченості користувачів цифрових пристроїв призводить до збільшення кібератак та витоку персональних даних. Зазначене свідчить про необхідність впровадження новітніх підходів щодо використання зазначеної технології та створення ефективних правових механізмів для захисту інформації. Таким чином, використання технологій ШІ повинно стати потужним інструментом у руках правоохоронних органів для протидії злочинності.

Крім цього, на нашу думку, вважаємо, що з метою вирішення зазначеної проблематики необхідно систематизувати існуючі підходів щодо можливостей використання технологій штучного інтелекту правоохоронними органами, акцентуючи увагу на міжнародному досвіді протидії злочинності. Зазначене дозволить забезпечити належний контроль та захист в контексті використання ШІ правоохоронними органами у ході проведення судово-експертної діяльності та досудового розслідування.

Таким чином, зосередження уваги на використанні правоохоронним органам ШІ допоможе безпечно та ефективно протидіяти злочинності, а також перейти до нового етапу розвитку стійкого цифрового майбутнього.

Список використаних джерел:

1. Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Safety, privacy, or both: Evaluating citizens' perspectives around artificial intelligence use by police forces. Policing and Society, doi:10.1080/10439463.2023.2211813.

2. Elsherif, M.S.A. The Legal Nature and Legality of Crime Prediction by Artificial Intelligen ce (2021) Arab Journal of Forensic Sciences and Forensic Medicine, 3 (2), pp. 341-359. DOI: 10.26735/NGSO4969.

3. Sachoulidou, A. (2023). Going beyond the "common suspects": To be presumed innocent in the era of algorithms, big data and artificial intelligence. Artificial Intelligence and Law, doi:10.1007/s10506-023-09347-w.

4. Trifonov, R., Nakov, O., Mladenov, V. (2019) Artificial intelligence in cyber threats intelligence. International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018, art. no. 8601235, Cited 10 times. DOI: 10.1109/ICONIC.2018.8601235.

5. Tabi, C., Hewage, C., Bakhsh, S. T., & Ukwandu, E. (2023). Contemporary issues in child protection: Police use of artificial intelligence for online child protection in the UK doi:10.1007/978-3-031-09691-4_5 Retrieved from www.scopus.com.

6. Ismail, J.I.M.S., Muhammad, M.N., Mosali, N.A. Ranking of Innovation Related Factors Influencing Artificial Intelligence Performance (2022) International Journal of Sustainable Construction Engineering and Technology, 13 (4), pp. 154-164. DOI: 10.30880/ijscet.2022.13.04.013.

7. Becker, S., Heuschkel, M., Richter, S., & Labudde, D. (2022). COMBI: Artificial intelligence for computer-based forensic analysis of persons. KI - Kunstliche Intelligenz, 36 (2), 171-180. doi:10.1007/s13218-022-00761-x.

8. Gans-Combe, C. (2022). Automated justice: Issues, benefits and risks in the use of artificial intelligence and its algorithms in access to justice and law enforcement doi:10.1007/978-3-031-15746-2_14 Retrieved from www.scopus.com.

Наукове видання

КУДІНОВ Вадим Анатолійович
ЯРОВИЙ Кирило Васильович та ін.

МАТЕРІАЛИ
міжвідомчого науково-практичного круглого столу на тему:

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ»

(*м. Київ, НАВС, 25 квітня 2024 року*)

Комп’ютерна верстка К.В. Ярового

Підписано до друку 13.05.2024. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 9,0. Ум. друк. арк. 8,37.
Тираж 300 прим.

Редакційно-видавничий центр
Національної академії внутрішніх справ
03035, Київ-35, пл. Солом’янська, 1

Друк: ФО-П Поліщук О.В.
Свідоцтво суб’єкта видавничої справи ДК №2142 від 31.03.2015
07400, м. Бровари, вул. Незалежності, 2, кв. 148
тел. (044) 592-13-49