МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Одеса
ОДУВС
2023

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. -- - 168 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2023 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов’язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад’юнктам), здобувачам вищої освіти першого та другого півня освіти.

Тому важливою складовою моделі професійної компетентності юриста є інформаційна компетентність, яка включає:

- компетентність у галузі інформаційних технологій, що полягає у використанні наданого багатого інструментарію не тільки для отримання інформації та її оброблення, але й для її подання у новій якості;

- компетентність у мережевих та комунікаційних технологіях, що характеризується не лише оперативним отриманням інформації, а й умінням організувати свою діяльність у якісно нових умовах, наприклад, створити власну юридичну консультацію в мережі Інтернет;

- аналітична компетентність, суть якої полягає в умінні на основі інформаційних технологій отримувати, узагальнювати та аналізувати професійно важливу інформацію.

Відповідно до загального розуміння феномену компетентності у сфері інформаційно-комунікаційних технологій, можливостей інформаційно-комунікаційних технологій для юридичної сфери можна подати визначення досліджуваного феномену: компетентність юриста в галузі інформаційно-комунікаційних технологій – це складна особистісно-професійна характеристика, що містить мотиваційно-проєктувальний компонент, що забезпечують гнучкість і готовність юриста адаптуватися до змін у професійній діяльності в умовах інформатизації суспільства, переміщати ідеї з галузі інформатики та інформаційних технологій в юридичну сферу при роботі з базами даних, різноманітних документів, а також прагнути до творчого самовираження з використанням можливостей інформаційно-комунікаційних технологій.

Серед ключових компетенцій, що становлять інформаційно-комунікаційну компетентність юриста, можна зазначити такі:

- інформаційну (характеризується способами прийому, зберігання та передачі);

- проєктувальну (характеризується способами визначення цілей, ресурсів, дій для їх досягнення, термінів здійснення);

- оцінну (характеризується способами порівняння, класифікації, абстрагування, прогнозування, систематизації, конкретизації інформації);

- комунікативну (характеризується способами передачі інформації та залучення ресурсів інших людей для досягнення своїх цілей).

Література:

1. Сіленко А. Інформаційні технології – новий імпульс для пошуку парадигми майбутнього суспільства. *Політичний менеджмент*. 2007. №3. С. 96–111.

2. Кадемія М. Ю., Шахіна І. Ю. Інформаційно-комунікаційні технології в навчальному процесі : Навчальний посібник. Вінниця: ТОВ «Планер», 2011. 220 с.

ОПТИМІЗАЦІЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ В КОНТЕКСТІ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Прохорчук Євген Олександрович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз
Одеський державний університет внутрішніх справ
Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

З усього обсягу інформації, за оцінками фахівців, аналізується лише 1%. Водночас інформація є корисною лише в тому випадку, якщо вона обробляється. Сьогодні навіть елементарне оброблення інформації людиною, наприклад перегляд, при величезному її обсязі просто фізично неможлива.

Саме такий стан спостерігається в правоохоронній сфері. Якщо недавно практичні всі відомості нагромаджувалися й оброблялися у файлах системи «Інформаційний портал Національної поліції України» (ІП НПУ) в структурованій регламентом формі, то зараз з інтенсивним впровадженням систем відеофіксації – це потокові відеодані, які в них

реєструються і обробляються в режимі on-line. Тому поліцейські у своїй роботі постійно використовують сучасні інформаційні технології, оскільки ефективність боротьби з правопорушеннями, і перш за все з кримінальними правопорушеннями, значною мірою залежить від інформаційного забезпечення діяльності правоохоронних органів [1].

І прикладом впровадження таких технологій у правоохоронній діяльності є створення автоматизованих інформаційних систем, які можна визначити як сукупність певним чином структурованих даних, що використовуються з метою здійснення тих чи інших видів правоохоронної діяльності, та комплексу апаратно-програмних засобів для зберігання даних та маніпулювання ними.

Як основні завдання створення системи автоматизованих систем можна назвати такі:

- сформувати та впровадити об'єднані банки даних для загального користування, які мають оперативно-довідкове, оперативно-розшукове, розшукове, криміналістичне, експертно-криміналістичне призначення, автоматизований облік суб'єктів, що підлягають дактилоскопічній реєстрації;
- забезпечити інформаційно-аналітичну діяльність усіх підрозділів правоохоронних органів;
- організувати обмін оперативно-службовою інформацією загального користування між правоохоронними органами в межах усієї держави, а за необхідності – й із зарубіжними країнами.

Для інформаційно-технологічного забезпечення діяльності органів поліції необхідне функціонування автоматизованих інформаційних систем за пріоритетними напрямами правоохоронної діяльності.

Залежно від призначення діяльності органів поліції застосовуються різні автоматизовані інформаційні системи. До них належать:

1) автоматизовані системи оброблення даних;
2) автоматизовані інформаційно-пошукові системи;
3) автоматизовані інформаційно-довідкові системи;
4) автоматизовані робочі місця;
5) автоматизовані системи управління;
6) експертні системи;
7) системи підтримки прийняття рішень та автоматизовані інформаційно-розпізнавальні системи.

Отже, інформаційні технології широко використовуються у діяльності поліції. Проте сьогодні вони потребують удосконалення, яке дозволить вивести правоохоронну діяльність на якісно новий рівень. Серед найбільш актуальних напрямів удосконалення інформаційних технологій у діяльності поліції на сучасному етапі можна виділити такі.

1. Використання технології «Big data», яка полягає в обробленні гігантських і зростаючих масивів даних та отриманні сприйнятих людиною результатів.

2. Використання технології «Deep learning». Глибокі нейронні мережі – це один із популярних підходів до створення різних систем штучного інтелекту в теперішній час. Успішність їх застосування зумовлена тим, що мережа автоматично виділяє з множини даних важливі ознаки, необхідні для виконання завдання.

3. Застосування методів нечітких множин прийняття оптимального юридичного рішення. Наприклад, вибір виду кримінального покарання або вибір запобіжного заходу в рамках досудового розслідування може базуватися на застосуванні методу аналізу ієрархій, що є складовою математичної теорії нечітких множин [3].

Запровадження нових інформаційних технологій та створення сучасних інформаційних систем, що дозволяють забезпечувати ефективну інформаційну підтримку на всіх рівнях управління правоохоронною діяльністю, - це ключове завдання, виконання якого необхідне для адекватного сучасним викликам та загрозам функціонування органів Національної поліції.

Література:

1. Швець Д.В. Ситуаційні центри НПУ як організаційна форма взаємодії підрозділів поліції при реагуванні на резонансні правопорушення. Застосування інформаційних технологій у

діяльності правоохоронних органів : мат. наук.-практ. семінару (м. Харків, 18 грудня 2019 р.). Харків: ХНУВС, 2019. С. 11–13.
2. Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС, затверджене наказом МВС України від 20.10.2017 № 870.
3. Желдак Т. А. Нечіткі множини в системах управління та прийняття рішень: навчальний посібник. Дніпро : НТУ ДП, 2020. 386 с.

ОСНОВНІ НАПРЯМИ РОЗВИТКУ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ
Бовтенко Денис Генадійович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз»
Одеський державний університет внутрішніх справ

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Питома вага кіберзагроз зростає. Ця тенденція за ступенем розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту найближчим десятиліттям посилюватиметься. Зростання такого впливу на функціонування структур управління, як національних, так і транснаціональних, формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів. [1, с. 140-145]

Кіберпростір – це новий канал для створення і поширення різноманітної інформації, він став новим двигуном зростання економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж і зовсім новою сферою державного суверенітету. Однак кіберпростір не тільки надає нам ресурси, можливості, але і містить загрози. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку, з якою стикаються люди, включаючи вразливих осіб, таких як діти. Для зменшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки у світі, щоб мережеві та інформаційні системи, комунікаційні мережі, цифрові продукти, послуги та пристрої, якими користуються громадяни, організації та підприємства – починаючи від малих та середніх до значних, що визначені в Рекомендації Комісії 2003/361/ЄС [2], для операторів критичної інфраструктури – краще захищені від кіберзагроз.

Кібернапади – це найбільші ризики, з якими може стикнутися будь-яка організація. За даними глобального огляду, проведеного об'єднанням ISACA, тільки 38% респондентів вважають, що вони підготовлені до кібернападів, решта, 83%, відносять кібернапади до однієї з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки [3]

Україна є однією з країн, які найбільше постраждали від кібератак. Під час російської агресії проти України кіберзагрози використовувалися як один із інструментів гібридної війни.

До об'єктів кібербезпеки належать конституційні права і свободи людини й громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури. Відповідно, до об'єктів кіберзахисту належать комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення сус-пільних потреб реалізації