

систем і баз. Тому наразі система захисту інформації потребує вдосконалення.

#### **Використані джерела:**

1. Беззубов Д.О. Інформаційна безпека органів внутрішніх справ у системі координації діяльності правоохоронних структур України // Міліція України: щомісяч. Інформ.-попул. та наук.-практ. ілюстр. журн. / співзасн. МВС України та Держ. ошад. Банк України. – 2012. - №5/6. – С. 18-19
2. Інформаційна безпека правоохоронних органів: Курс лекцій / О.В. Рибальський, В.Г. Хахановський, Ю.Ю. Орлов та ін.. – К.: Нац. акад. внут. справ, 2004.-148с.
3. Бойченко О.В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : монографія / О.В. Бойченко. – Сімферополь: ВАТ «Сімферопольська міська друкарня», 2009. – 288 с.

**Дума А.** курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ  
**Науковий керівник: Рижков Е.В.**  
к.ю.н. , доцент, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

### **ІНФОРМАЦІЙНА БЕЗПЕКА НАЦІОНАЛЬНОЇ ПОЛІЦІЇ**

Процес інформатизації діяльності територіальних органів поліції України тягне за собою широкі можливості доступу до інформаційних ресурсів, які використовуються в діяльності поліції щодо забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку. Тому підвищення ефективності діяльності Національна поліція України може бути вирішено через запровадження надійної системи інформаційної безпеки.

О. Красікова вважає, що інформаційну безпеку Національної поліції України можна досягти тільки за двома формами: організована котра полягає в організації роботи поліції пов'язаної з збиранням, обігом, обробкою, зберіганням та використанням інформації та взаємодії працівників; правова форма полягає у створенні інструкцій та положень, складання планів чи навіть виданні розпоряджень та наказів [1, с. 20].

Тому можна стверджувати, що інформаційна безпека Національної поліції

України полягає у її спроможності забезпечити інформаційні ресурси від несанкціонованого доступу до них.

На даний час основним напрямом протидії витоку інформації є забезпечення фізичного (технічні засоби, лінії зв'язку, персонал) та логічного (операційна система, прикладні програми, дані) захисту інформаційних ресурсів органів поліції України. При цьому безпека досягається завдяки використанню апаратних, програмних та криптографічних методів та засобів захисту, а також комплексом організаційних заходів.

Але незважаючи на значні результати в області інформатизації та запровадження новітніх інформаційних технологій в діяльність поліції кінцева ефективність забезпечення інформаційної безпеки не завжди відповідає сучасним вимогам [2]. Сучасні системи безпеки мають високі характеристики тільки по окремим напрямам забезпечення безпеки. Прямолінійне вирішення даної проблеми шляхом створення на кожен інформаційну систему власної системи безпеки не є ефективним та не забезпечує можливості практичної реалізації на всіх рівнях, а саме: фінансові обмеження, складність в експлуатації та координації дій. Логічним виходом з цієї ситуації є інтеграція окремих інформаційних систем та систем безпеки [3, с. 102].

У сфері інформаційної безпеки України вирізняються такі життєво важливі інтереси держави: недопущення інформаційної залежності та блокади України, інформаційної експансії з боку інших держав та міжнародних структур; ефективне функціонування механізму взаємодії органів державної влади та інститутів громадянського суспільства при виробленні, реалізації та коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства як необхідної передумови конкурентоспроможності України в сучасному світі; забезпечення економічного та науково-технологічного розвитку України; формування позитивного іміджу України; організація системи захисту прав громадян на вільний і безперешкодний доступ до інформації, залучення їх формування системи інформаційної безпеки; інтеграція України у світовий інформаційний простір.

Тому розглянувши основні чинники котрі впливають на інформаційну безпеку Національної поліції України, ми сформуваємо основні положення котра на нашу думку будуть доцільними: законодавчий чинник полягає в ухваленні нормативно-правових актів, за допомогою котрих можна встановити правила використання й обробки інформації, доступ до якої обмежено, та визначають ступінь відповідальності за порушення цих правил; технічний чинник допомагає регулювати доступ до всіх ресурсів інформаційної системи, а саме: технічної, програмної, елементів баз даних), регламентація порядку роботи користувачів і персоналу.

Таким чином, система інформаційної безпеки має бути спрямована на запобігання втрати інформації, її перекручення, несанкціонованого доступу та незаконного її використання під час проектування, впровадження та експлуатації інформаційних підсистем. Безпека та захист в інформаційних системах Національної поліції має будуватись з урахуванням комплексного підходу до побудови системи захисту, що передбачає об'єднання в єдиний комплекс необхідних

заходів та засобів захисту інформації на всіх рівнях системи інформаційного забезпечення.

#### **Використані джерела:**

1. Красіков Д.О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.19 К., 2019. 20 с.

2. Іванець Т.М. Інформаційна безпека держави як умова для збереження національного суверенітету. [Електронний ресурс]. – Режим доступу: <http://intkonf.org/ivanets-tm-informatsiyna-bezpeka-derzhavi-yak-umova-dlya-zberezhennyansionalnogo-suverenitetu/> (дата звернення: 12.11.2020).

3. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України № 537V від 9 січня 2007 р. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

**Філімонов В.О.** курсант 2 курсу ФПФОДР

Дніпропетровського державного  
університету внутрішніх справ

**Науковий керівник: Рижков Е.В.**

завідувач кафедри, кандидат юридичних наук,  
доцент кафедри економічної та інформаційної  
безпеки Дніпропетровського державного  
університету внутрішніх справ

### **ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ЧЕРЕЗ ГЕОІНФОРМАЦІЙНУ СИСТЕМУ**

У даній роботі розглянуто поняття та сутність геоінформаційної системи, її структура та основні функції, можливості її вдосконалення шляхом прийняття певних законів та нормативно-правових актів, що будуть слугувати регулятором взаємовідносин між громадянами, їх власністю кіберполіцією України.

Сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційного забезпечення та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Це явне підтвердження загальновідомої тези "хто володіє інформацією, той володіє світом" .

Необхідним заходом управління є наявність вичерпної, цілком достовірної, позбавленої суб'єктивних ( неточних повністю та офіційно не підтверджених) слів інформації, яка необхідна для виконання певної конкретної задачі та допускає прийняття відповідного, добре продуманого управлінського рішення. Ця інформація повинна відображати не тільки реальний стан справ, але й тенденції,