Серенок. – Вінниця : ГО «Подільська агенція регіонального розвитку», 2014. – 86 с. – Режим доступу: http://nc.gov.ua/news/index.php?ID=1577.

5. Сучасний стан, проблеми і перспективи розвитку в Україні електронних адміністративних послуг. [Електронний ресурс]. – Режим доступу: http://www.euroosvita.net/prog/print.php/prog/print.php?id=3808

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

## ІНФОРМАЦІЙНА БЕЗПЕКА В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Під інформаційною безпекою слід розуміти стан захищеності національних інтересів України в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства і держави. Досвід останній років показує, що Україна зовсім не готова протидіяти атакам в інформаційній сфері. Водночас застосування інформаційних технологій є вимогами часу, які дозволяють швидко й точно збирати дані, оперативно вирішувати завдання щодо зміцнення правопорядку та законності, а також є запорукою протидії злочинності. Саме необхідністю створення механізмів захисту інформації, що використовуються правоохоронними органами, і зумовлена актуальність дослідження.

Сформулюємо визначення інформаційної безпеки органів внутрішніх справ (далі – ОВС) – це стан інформації щодо діяльності ОВС України, при якому з нею ознайомлені лише суб'єкти, які передбачені чинним законодавством та виключено можливість надходження інформації до третіх осіб [1, с.18]. Тобто інформаційна безпека в органах Національної поліції України має на меті збереження цілісності інформації, що циркулює в поліції, і має деякі особливості. В першу чергу це стосується інформації, що містить державну таємницю. Відзначимо, що державна таємниця – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці

України та які визнані державною таємницею та підлягають охороні державою [2, с.7].

Треба сказати, що захист інформації не є основною функцією правоохоронних органів України, тому їхня діяльність не спрямована на забезпечення власної інформаційної безпеки. Така ситуація складається в результаті того, що на сьогодні не існує єдиної системи служб і підрозділів, робота яких була б спрямована на забезпечення такого захисту. Вважаю за необхідне створення такої системи для захисту інформації, що використовується правоохоронними органами при здійсненні покладених на них повноважень, від несанкціонованого доступу та незаконного її використання.

Загалом політика інформаційної безпеки має бути спрямована на мінімізацію та, по можливості, уникнення існуючих чи потенційних внутрішніх або зовнішніх загроз розвитку інформаційно-аналітичного забезпечення ОВС відповідно до її цілей [3, с.9].

Пропонуємо виділити наступні форми гарантування інформаційної безпеки ОВС:

– законодавчий, що включає ухвалення нормативно-правових актів, які встановлюють правила використання й обробки інформації, доступ до якої обмежено, та визначають ступінь відповідальності за порушення цих правил;

– технічний, що полягає у регулюванні доступу до всіх ресурсів інформаційної системи (технічних, програмних, елементів баз даних), регламентації порядку роботи користувачів і персоналу.

Досвід правоохоронних органів інших країн щодо забезпечення інформаційної безпеки дозволяє виокремити два основні напрями. Один із них полягає в удосконаленні діяльності правоохоронних органів щодо гарантування власної інформаційної безпеки зсередини. Інший – у покращенні правового забезпечення інформаційної безпеки на державному рівні.

Треба відзначити, що для досягнення вищого рівня забезпечення інформаційної безпеки правоохоронних органів необхідним є не тільки вдосконалення чинного законодавства, а й наявність механізму його втілення в життя. За такого підходу, на нашу думку, можливо активізувати всі фактори, необхідні для гарантування інформаційної безпеки нашої держави.

До основних принципів органів внутрішніх справ у сфері захисту інформації належать: єдність підходів до забезпечення захисту інформації; комплексність, повнота і безперервність заходів в питаннях захисту інформації; відвертість нормативно-правових актів і нормативних документів з питань захисту інформації, які не містять відомостей, складових державної таємниці; обов’язковість захисту інженерно-технічними засобами інформації, яка складає державну та іншу, передбачену законом, таємницю; конфіденційність інформації, що є власністю держави та відомства.

Отже, треба підсумувати, що аналіз роботи органів та підрозділів Національної поліції свідчить про те, що однією з проблем попередження, виявлення та розкриття злочинів є недостатній рівень захищеності відомчих інформаційних мереж та систем, доступ до інтегрованих інформаційно-пошукових

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

**Використані джерела:**

1. Беззубов Д.О. Інформаційна безпека органів внутрішніх справ у системі координаії діяльності правоохоронних структур України // Міліція України: щомісяч. Інформ.-популя. та наук.-практ. ілюстр. журн. / співзасн. МВС України та Держ. ощад. 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