правове регулювання сфери інформаційного забезпечення правоохоронних органів.

Список використаних джерел:

1. Снегірьова Т. Л. Інформаційні технології в діяльності правоохоронних органів та необхідність їх вивчення курсантами вищих навчальних закладів системи МВС. URL: http://bo0k.net/index.php?p=achapter&bid.

2. Бочковий О.В. Ігнорування інформаційно-технічного прогресу органами досудового розслідування в Україні: хронічна риса чи тимчасове явище? Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2016. Вип. 3. С. 223–231.

3. Хорт І.В. Особливості інформаційного забезпечення органів внутрішніх справ у сфері охоронної діяльності / І. В. Хорт // Наукові праці МАУП, 2015. Вип. 44(1). С. 100–107.

4. Криміналістика: підручник / [В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель та ін.] ; за ред. В.Ю. Шепітька. – 5-те вид. переробл. та доповн. Київ : Ін-Юре, 2016. 640с.

УДК: 351.74:004.9

ДІАНА АРТУРІВНА ТУПОТІНА
курсант 2 курсу факультету підготовки фахівців досудового розслідування Дніпропетровського державного університету внутрішніх справ
НАТАЛІЯ СЕРГІЇВНА РЕЗЦОВА
викладач кафедри кримінального процесу Дніпропетровського державного університету внутрішніх справ, майор поліції

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

У міру розвитку і ускладнення комп'ютерних систем і програмного забезпечення зростає обсяг і підвищується вразливість даних, які зберігаються в них. Тому все більшої уваги набувають проблеми захисту інформації. Важлива роль захисту інформації випливає з розуміння того, що захист інформації є не тільки однією з головних складових національної безпеки держави, а й невід'ємним компонентом всіх її складових; інформаційні стратегії в сучасних умовах набувають важливого значення під час реалізації різних моделей співробітництва, захисту населення та дотримання законності або відіграють роль своєрідної "інформаційної зброї"; руйнування та дезорганізація інформаційної інфраструктури держави прирівнюються за наслідками до застосування зброї масового знищення; витік інформації в процесі діяльності органів внутрішніх справ призводить до зростання злочинності, її безкарності та зневіри населення тощо.

Інформація повинна бути захищеною як правовими актами, так і технічними засобами. [1]

Захист інформації особливо важлива проблема в умовах інформаційного суспільства. Проблемою технічних засобів захисту інформації у свій час займались такі українські вчені: Ю. Добути, О. Рибальський, І. Горбенко, В. Захаров, Г. Гулак, В. Хорошко, Ю. Орлов, О. Потій, Ю. Горбунко та інші.

Ідею захисту інформації в контексті економічної безпеки регіону за допомогою тільки технічних засобів в умовах інформаційного суспільства не можна вважати достатньо ефективною. Цей напрямок можна посилити математичними і методами, істотно при використанні криптографічних алгоритмів. Запропоновано електронно-криптографічний систему і алгоритми виконання, використовують елементи штучного інтелекту для захисту інформації. Таким чином, авторами запропоновано проект малогабаритного шифрувального пристрою, який може бути застосований у практичній діяльності оперативних підрозділів, особливо в тих випадках, коли є підозра, що в процесі проведення оперативно-розшукових заходів або операцій можуть прослуховуватись розмови оперативних працівників.

На даний час, за оцінкою Міжнародного союзу електрозв'язку, Республіка Білорусь за підсумковим індексом розвитку інформаційно-комунікаційних технологій (ІКТ) піднялася з 52-го місця в 2011 року на 31-е в 2016 р серед 175 країн. За даний період в Білорусі створено базовий комплекс електронного уряду, в який входять такі компоненти, як загальнодержавна автоматизована інформаційна система, система міжвідомчого електронного документообігу, державна система управління відкритими ключами перевірки електронного цифрового підпису, єдиний розрахунковий інформаційний простір. [2] Відповідно до Концепції національної безпеки Республіки Білорусь, одним з основних національних інтересів в інформаційній сфері є забезпечення надійності та стійкості функціонування критично важливих об'єктів інформатизації.

Виходячи з викладеного, представляється необхідним стратегічне управління інформаційною безпекою в правоохоронній сфері розглядати в якості унікальної системи, яка повинна своєчасно розпізнавати проблеми, висувати науково-обгрунтовані стратегічні цілі, шляхи та способи їх досягнення; формувати уявлення про стан системи в майбутньому зі збереженням традиційних і придбанням (створенням) нових здібностей і можливостей управління, своєчасно вловлювати і розпізнавати можливості і загрози, що виходять із зовнішнього середовища; виробляти способи зміни зовнішнього оточення, реформування правоохоронної сфери, системи оперативного управління в міру збільшення власного потенціалу, виконання стратегічних завдань.

Список використанної літератури:

1. Варенко В.М. Інформаційно-аналітична діяльність. Навч. посіб. Київ: Університет «Україна», 2014. 417 с.

2. Інформаційні технології в правоохоронній діяльності. Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, В.А. Іщенко: НАВСУ, 2013. 82с.

3. Проект закон України «Про технічний та криптографічний захист інформації»URL:http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=2D026D15A28D130D7C40D9F2186DF6AE?art_id=73862&cat_id=38837

УДК 343.9[343.346.8:004](477)

ВОЛОДИМИР АНАТОЛІЙОВИЧ ЄВТУШОК
старший викладач кафедри тактичної та спеціальної фізичної підготовки Харківського національного університету внутрішніх справ, підполковник поліції

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ДЛЯ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ

Метою роботи є дослідження питання впровадження сучасних інформаційних технологій для підвищення ефективності боротьби зі злочинами, вчиненими з використанням комп'ютерних та мережевих можливостей.

З урахуванням збільшення чисельності користувачів, мережа Інтернет закономірно породжує залежність людей від інформаційного співтовариства і вразливості від різного роду кіберзлочинів. Сучасні інформаційні технології займають в економіці країни особливе місце, а їх ефективне функціонування є одним з найважливіших факторів, які сприяють вирішенню ключових завдань політики. Необхідно звернути увагу на виявлення, розкриття і розслідування злочинів, скоєних в кіберпросторі. Поширення комп'ютерних вірусів, шахрайства з платіжними картами, розкрадання грошових коштів з банківських рахунків, комп'ютерної інформації, порушення правил експлуатації автоматизованих електронних систем, різного роду протиправні дії з використанням криптовалют - далеко не повний перелік злочинів, скоєних за їх допомогою. Великою проблемою є те, що інформація індивідуальна, ірраціональна та анонімна, а кожна людина в сучасному світі, від звичайного робітника до великої компанії, банку і держави, ризикує в будь-який момент стати жертвою зловмисників в кіберпросторі. Отже постійно винаходять нові, складні та різноманітні схеми шахрайських операцій.

З настанням нового століття рішенням таких злочинів стало приділятись багато уваги як на національних рівнях, так і в рамках реалізації програм міжнародного співробітництва державних правоохоронних органів. Головна криміналістична особливість кіберзлочинів полягає в тому, що їх запобігання, виявлення, розкриття і розслідування неможливо без використання сучасних інформаційних технологій. На жаль теперішня