

Незважаючи на недоліки технології, вона має бути застосована у діяльності Національної поліції України.

Одержано 17.04.2019



УДК 343.9;681.5

Вікторія Олександрівна КОВТУН,

курсант групи Ф4-102 ХНУВС

Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Активне застосування Національною поліцією України в правоохоронній діяльності безпілотних літальних апаратів (БпЛА) потребує проведення наукових досліджень щодо нормативного врегулювання цього процесу. Використання БпЛА в зазначеній сфері може мати процесуальний, організаційний, оперативний чи профілактичний характер. Правове регулювання застосування пов'язано з питанням нормативно-правового регулювання в оперативно-розшуковій діяльності та під час досудового розслідування. Вказаний напрям досліджувало чимало науковців, серед яких О. М. Бандурка, В. І. Василичук, Л. І. Громовенко, О. Ф. Долженков, Ю. Ф. Жаріков, І. П. Козаченко, Я. Ю. Кондратьєв, Д. Й. Никифорчук, Ю. Ю. Орлов, В. Л. Ортинський, О. П. Снігєрьов, І. Ф. Хараберюш та ін.

Застосування в правоохоронній діяльності БпЛА має бути узгоджено з Міністерством оборони України. Варто зауважити, що на БпЛА поширюються всі вимоги, які висувають до використання повітряних суден, якщо в законодавстві не сказано інакше.

До напрямків використання БпЛА у діяльності Національної поліції України можна віднести:

1) протидія злочинності:

- для проведення візуальної розвідки з метою виявлення можливих загроз для людей та правоохоронців, наприклад, виявлення місця перебування зловмисників на певній території чи в будівлі, встановлення чи озброєні вони та чим саме;

- виявлення місць відстою вантажівок з товаром, що був незаконно завезений на територію України, або обіг якого заборонений в Україні;

- виявлення місць незаконних посівів нарковмісних рослин;

- передача відеосигналу та фотографій для подальшого розпізнавання осіб і номерних знаків автомобілів, які перебувають у розшуку;

- дистанційне обстеження підозрілих предметів (наприклад, пакетів або сумок) з метою проведення первинної оцінки щодо належності цих предметів до вибухових пристроїв;

2) в пошуково-рятувальних операціях, у тому числі в нічний час, наприклад, для пошуку осіб:

- які загубились;
- постраждали в наслідок аварій техногенного чи природного характеру;

3) під час забезпечення публічної безпеки та порядку:

– у місцях масового скупчення людей, наприклад, для виявлення та своєчасного припинення протиправних дій шляхом звернення через гучномовець до осіб, які вчиняють протиправні дії з вимогою припинити правопорушення;

– на автошляхах та автомагістралях для виявлення та аналізу дорожньо-транспортних пригод, шляхів проїзду до місця події.

Наведений перелік не є вичерпним.

Одержано 13.04.2019



УДК 004.047

Максим Володимирович КОРЖОВ,

курсант групи Ф4-102 ХНУВС

Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

У сучасному світі надзвичайно важливою є проблема захисту інформації. На даний момент можна придбати інформацію із соціальних мереж будь-якого користувача. Будь-що викладене в Інтернет залишиться там назавжди. Блокувати інформацію не має сенсу, адже блокування дуже легко обійти використовуючи Proxy-сервери. Існує величезна кількість кібератак, крадіжок грошей із карток з технологією безконтактної оплати. Це значно відображується на суспільстві та загрожує кожному. Технології та методи, які використовують зловмисники модернізуються, а сучасна ієрархічна структура не дозволяє поліцейським ефективно та своєчасно відповідати на виклики сьогодення. Те, що працювало місяць тому, сьогодні може виявитися застарілим та малопридатним для застосування у практичній діяльності.

Злочини у кіберпросторі не тільки важко зафіксувати, їх треба довести юридично. Реформувати систему інформаційної безпеки до того рівня, щоб можна було вирішити усі питання майже неможливо, тому треба не допускати можливості скоєння злочинів заздалегідь:

- важливими є освітні проекти з медіа-грамотності;
- треба привертати увагу громадськості до захисту особистої інформації;
- рекомендувати власникам карток з технологією безконтактної оплати класти до гаманця фольгу, щоб та закривала RFID мітку;
- створити окремі додатки з актуальною інформацією в галузі інформаційних технологій та кібербезпеки, переймати міжнародний досвід;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії