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 вчинять 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

комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань.

Особливу увагу треба привертати підготовці особового складу НПУ до змін у загальній системі інформаційного забезпечення, а також навчання співробітників нових підрозділів грамотному використанню інформаційних систем для вирішення оперативно-службових завдань;

Також, система інформаційної безпеки має бути більш гнучкою. Треба розробляти нові методи, більш зручні у використанні, які охоплюють всі напрямки практичної діяльності НПУ. А саме збір, обробку та узагальнення оперативно-довідкової, аналітичної, статистичної та контрольної інформації для оцінки ситуації та прийняття обґрунтованих рішень на всіх рівнях управління НПУ.

Надзвичайно важливим є облік запитів поліцейських для запобігання корупції, продажу інформації з обмеженим доступом, тому він має відповідати певним критеріям захисту, таким як: двосторонній ключ або індивідуальний пароль, що має різні символи, цифри і букви, та закріплюється на певний строк.

Вирішення цих та інших завдань сприятиме створенню сучасної інформаційної системи НПУ, що сприятиме реалізації державної політики у сфері реформування системи правоохоронних органів, боротьби зі злочинністю та зменшенню кількості кібератак.

Одержано 19.04.2019

УДК 332.012+004.056

Ксенія Олександрівна КРАТАСЮК,
курсант групи Ф4-302 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ВИКОРИСТАННЯ ДИСТРИБУТИВУ KALI LINUX У КІБЕРБЕЗПЕЦІ

На сьогоднішній день дистрибутив KaliLinux набирає велику популярність. Можливості KaliLinux зосереджені на тестуванні безпеки, це є великою перевагою над іншими операційними системами, але в той же час KaliLinux може бути використано хакерами з метою пошуку вразливостей у вашій системі – це являється недоліком дистрибутива.

Відмінності Linux від системи Windows полягає в тому, що Linux – відкритий та безкоштовний продукт, не потрібно платити за антивірусне програмне забезпечення, яке споживає багато системних ресурсів і робить ваш ПК повсякденним і потребує регулярного оновлення. Більшість LinuxDistribution має власний центр програмного забезпечення, з якого можна легко його встановити.