підписане електронним підписом, направляє оператору мобільного зв'язку і черговому по місту. Оператор мобільного зв'язку, отримавши запит на інформацію і дозвіл від судді, надає її оперативному черговому міста. Існують різне програмне забезпечення, наприклад PGP програма, яка може забезпечити описаний алгоритм.

Таким чином, розглянуті методи дозволять істотно скоротити час реагування на події.

Одержано 17.04.2018

УДК 623.094

Вікторія Володимирівна ДЕСЯЦЬКА,
курсант групи Ф4-202 ХНУВС
Науковий керівник: доцент кафедри інформаційних технологій факультету № 4 ХНУВС кандидат технічних наук, доцент Мордвинцев М. В.

ВИКОРИСТАННЯ КВАДРОКОПТЕРІВ У ПОЛІЦЕЙСЬКІЙ ДІЯЛЬНОСТІ

Квадрокоптери набувають все більшого поширення в Україні. Квадрокоптери використовують як хобі, широко використовуються в комерційних цілях, проводяться спортивні змагання на дронах.

Збільшилася кількість злочинів з їх використанням:

– нелегальне спостереження за приватним життям людей;
– розвідка об'єктів потенційного грабежу;
– установка і використання на квадрокоптери вогнепальної зброї;
– установка на квадрокоптери бомб і гранат;
– використання квадрокоптера для проведення терактів зі знищенням пасажирських літаків.

Для зменшення кількості злочинів, катастроф літаків, травм людей в країнах Європи прийнято ряд законів обмежують використання дронів. У різних країнах вони дещо відрізняються один від одного, але в основному дуже схожі.

До них відносять:

– використання дронів передбачається тільки в умовах прямого візуального контакту дистанційного пілота;
– максимальна швидкість польоту – 150 км / год;
– максимальна висота польоту 120 метрів над рівнем землі і 500 метрів від дистанційного пілота, якщо не задіяний візуальний спостерігач;
– дронам забороняється виконувати польоти в 8-кілометровому периметру аеропорту, а також в заборонених зонах;
– всі польоти БПЛА не повинні виконуватися над людьми, крім дистанційного пілота;
– польоти повинні виконуватися тільки в світлий час;
– на дронах повинні бути відсутніми небезпечні матеріали, крім елементів живлення.
– дистанційний пілот повинен гарантувати нормальний фізичний і психологічний стан для безпечної експлуатації (вживання алкоголю або втома).

Для потреб органів внутрішніх справ квадрокоптер можна використовувати в наступних цілях:

– планове спостереження за ситуацією в місцях великого скупчення людей, таких як стадіони, мітинги, концертні майданчики;
– оперативне реагування на вчинений злочин і відстеження переміщень зловмисника;
– обстеження об'єктів на предмет наявності підозрілих предметів;
– пошук зниклих громадян, особливо в важкодоступній місцевості;
– відстеження дорожньої ситуації на міських і заміських магістралях з метою прийняття рішення по перенаправлення трафіку;
– доставка термінових вантажів для співробітників поліції або людей, що потрапили в біду;
– чергове спостереження за дорученим районом в денний і нічний час;
– пошук підозрюваних в скоєнні правопорушень в певному районі.

Ці факти говорять про те, що поліція України повинна бути оснащена квадрокоптерами. Причому ці пристрої повинні мати більш високими технічними характеристиками, що дозволить мати переваги в боротьбі зі злочинцями. Для цього повинні створюватися центри підготовки пілотів з урахуванням специфіки роботи поліції.

Одержано 17.04.2018

УДК 004.9

Данило Олексійович КУЛІКОВ,
курсант групи Ф4-202 ХНУВС
Науковий керівник: старший викладач кафедри інформаційних технологій факультету № 4 ХНУВС Кубрак В. П.

СИТУАЦІЙНІ ЦЕНТРИ НПУ ЯК ОРГАНІЗАЦІЙНА ФОРМА ВЗАЄМОДІЇ ПІДРОЗДІЛІВ ПОЛІЦІЇ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БОРОТЬБИ З ПРАВОПОРУШЕННЯМИ

Ефективність боротьби з правопорушеннями, і перш за все з кримінальними, в значній мірі залежить від інформаційного забезпечення діяльності правоохоронних органів.

В умовах стрімкого зростання інформаційних потоків і недостатність часу для прийняття необхідних управлінських заходів важливим стає створення сучасного науково-технологічного підрозділу, який сприяє оперативному

інформаційно-аналітичному забезпеченню діяльності правоохоронних органів і прийняттю своєчасних ефективних управлінських рішень.

Такими підрозділами є Ситуаційні центри Національної поліції України (СЦ). При цьому під центром розуміється не лише спеціально обладнане приміщення, але і відповідні інформаційні, телекомунікаційні, програмні та методичні засоби з метою вироблення відповідних управлінських рішень.

Співробітники правоохоронних органів у своїй роботі постійно використовують сучасні технології. І чим більше цих технологій, тим складнішим стає процес їх об'єднання і інтеграції.

Тому рішенням цієї проблеми стає об'єднання існуючих потоків інформації і інструментів управління в єдиний інформаційний візуальний простір на базі геоінформаційних системи (ГІС). Подібні рішення дозволяють повноцінно організувати збір необхідної інформації, її обробку, аналіз і надання доступу до результатів обробки.

Впроваджуючи геоінформаційні системи в роботу ситуаційних центрів, поліція отримує програмну платформу для реалізації ефективного управління та реагування в справі охорони громадського боротьби з правопорушеннями. ГІС з самого початку створювалися для збору, аналізу і відображення даних в найбільш зрозумілому людині вигляді: шляхом нанесення на карту.

Ситуаційні центри надають наступні можливості:

– Оперативний доступ до легкої для розуміння карти з виводом необхідної інформації, з використанням різних каналів передачі даних.

– Збір, зберігання і обробка даних про злочини, правопорушників, підозрюваних, місцях підвищеної небезпеки і будь-яких інших типах об'єктів.

– Надання результатів аналітичної роботи для виявлення залежності між кримінально значущою інформацією і прогнозованими ризиками при плануванні оперативно-розшукових заходів.

– Підвищення ефективності планування і прийняття управлінських рішень.

Ситуаційний центр, перш за все, побудований на аналізі ситуації. За словами начальника Департаменту організаційно-аналітичного забезпечення та оперативного реагування МВС України полковника поліції Сергєєва О.О. у Національній поліції України використовують три види аналізу. Стратегічний (кримінологічний) – аналіз злочинності, її рівня, поширеності, динаміки, структури загалом. Проводиться аналіз стану злочинності в країні, визначається, в яких регіонах складна криміногенна ситуація, і що потрібно робити, щоб стабілізувати обстановку. Другий рівень – тактичний аналіз. Це ситуація впродовж доби, тижня щодо конкретних регіонів, конкретних видів злочинів. Саме цим і займаються ситуаційні аналітики. Третій рівень (один із найскладніших) – практичний. Це оперативний кримінальний аналіз. Це робота щодо кожного конкретного тяжкого та особливо тяжкого злочину.

Одержано 17.04.2018

УДК 342.922

Дмитро Олександрович РУДЕНКО,
Андрій Олександрович ЛАЩЕНКО,
студенти групи КБдср-17-1 ХНУВС
Науковий керівник: завідувач кафедри інформаційних технологій факультету № 4 ХНУВС кандидат технічних наук, доцент Струков В. М.

ВИКОРИСТАННЯ АКТИВНИХ МЕТОДІВ ВТОРГНЕННЯ У КОМП'ЮТЕРНІ МЕРЕЖІ

Серед активних методів виявлення вторгнення у комп'ютерні мережі одним з найбільш широко використовуваних є так звані сніфери.

Аналіза́тор тра́фіку, або сні́фер (від англ. *to sniff* – нюхати) – програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів.

Перехоплення трафіку може здійснюватися:

– звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), інакше метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);

– підключенням сніфера в розрив каналу;

– відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;

– через аналіз побічних електромагнітних випромінювань і відновлення трафіку, що таким чином прослуховується;

– через атаку на канальному (MAC-spoofing) або мережевому (3) рівні (IP-spoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

На початку 1990-х широко застосовувався хакерами для захоплення призначених для користувача логінів і паролів, які у ряді мережевих протоколів передаються в незашифрованому або слабозашифрованому вигляді. Широке розповсюдження хабів дозволяло захоплювати трафік без великих зусиль у великих сегментах локальної мережі практично без ризику бути виявленим.

Сніфери застосовуються як в цілях профілактики та протидії кібератакам, так і в деструктивних цілях.

Аналіз трафіку, що пройшов через сніфер, дозволяє:

Виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним устаткуванням і її подальший аналіз).

Виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніферів – моніторів мережної активності).