УДК 65.012.8 + 004
ДМИТРО ВОЛОДИМИРОВИЧ ШВЕЦЬ
Ректор Харківського національного університету внутрішніх справ
кандидат педагогічних наук, доцент, полковник поліції

СИТУАЦІЙНІ ЦЕНТРИ НПУ, ЯК ОРГАНІЗАЦІЙНА ФОРМА ВЗАЄМОДІЇ ПІДРОЗДІЛІВ ПОЛІЦІЇ ПРИ РЕАГУВАННІ НА РЕЗОНАНСНІ ПРАВОПОРУШЕННЯ

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

Співробітники правоохоронних органів у своїй роботі постійно використовують сучасні інформаційні технології. І прикладом впровадження таких технологій є створення ситуаційних центрів.

Тому дослідження впровадження новітніх інформаційних технологій у діяльність НПУ є досить актуальною задачею.

Метою даної доповіді є аналіз методів та засобів побудови та функціонування ситуаційних центрів НПУ.

Ситуаційний / диспетчерський центр – це приміщення (зал, кімната, кабінет), оснащене засобами комунікацій (відеоконференцзв'язок, конференц-зв'язок та іншими засобами інтерактивного представлення інформації), призначене для оперативного прийняття управлінських рішень, контролю і моніторингу об'єктів різної природи, ситуацій і інших функцій.

При цьому під центром розуміється не лише спеціально обладнане приміщення, але і відповідні інформаційні, телекомунікаційні, програмні та методичні засоби з метою вироблення відповідного управлінського рішення.

Таким чином, *ситуаційний центр* – це, передусім, сукупність спеціальних інформаційних технологій та апаратно-програмних комплексів, що реалізовують функції підготовки управлінських рішень з урахуванням оцінки їх наслідків, причому процес розробки і прийняття рішення відбувається в реальному часі по відношенню до тих подій, на які треба реагувати.

Основними завданнями ситуаційних / диспетчерських центрів є:

– моніторинг стану об'єкта управління з прогнозуванням розвитку ситуації на основі аналізу інформації, що надходить;

– моделювання наслідків управлінських рішень, на базі використання інформаційно-аналітичних систем;

– експертна оцінка прийнятих рішень і їх оптимізація;

– управління в кризовій ситуації.

Основними елементами технічного оснащення ситуаційного / диспетчерського центру є:

– комп’ютерна мережа, що дозволяє вводити, обробляти, зберігати і передавати інформацію за напрямком діяльності ситуаційного центру;

– екран колективного користування (відеостіна, проекційна установка) Екран колективного користування - це система мультіекранного відображення даних різного виду (відеозображення, електронні карти, графіки та діаграми, текстова документація в електронному вигляді). Завдяки модульній конструкції система може конфигурироваться індивідуально під конкретні приміщення і завдання. Ключовою властивістю екрану колективного користування є дозвіл і, відповідно, інформаційна ємність, що дозволяє представляти на одному екранному полі безліч «вікон», що містять повноцінні зображення від різних джерел;

– засоби відеоконференцзв'язку які грають одну з ключових ролей в ситуаційному центрі, забезпечуючи проведення колективних нарад між віддаленими учасниками обговорення. У разі виникнення надзвичайних ситуацій в ситуаційному центрі організовується безпосереднє мовлення з місця події. Дане рішення необхідно не тільки для міністерств з надзвичайних ситуацій, але для транспортних і видобувних компаній;

– система звукооснащення зазвичай включає конференц-систему, призначену для проведення групових обговорень. При цьому кожне робоче місце учасника нарад в ситуаційному / диспетчерському центрі оснащується окремим мікрофоном (мікрофонним пультом) для виступів. Система звукооснащення також включає системи посилення (мікшування) звуку і акустичні системи;

– допоміжне обладнання, яке включає в себе електронні засоби введення і відображення графічних даних, такі як документ-камери, інтерактивні дошки та ін.;

– інтегрована система управління ситуаційного / диспетчерського центру забезпечує взаємодію всіх елементів технічного оснащення. В силу високої складності система управління зазвичай вимагає постійної присутності обслуговуючого персоналу.

Ситуаційний центр, як правило, розміщується на базі окремого підрозділу, в якому є прямий доступ не тільки до різних джерел інформації, але і до всіх ключових співробітників, включаючи керівництво і конкретних виконавців.

Ключовим компонентом СЦ має бути потужна багатофункціональна геоінформаційна система (ГІС).

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

Подібні ГІС системи можуть інтегруватися з ситуаційними центрами загальнодержавного, обласного чи міського призначення, для підключення раніше недоступних або непридатних наборів даних. В результаті сумісних досліджень можна отримати більш повну картину злочинності, поліпшити

тактику реагування та розслідування, значно спростити щоденні завдання. В результаті, процес прийняття рішень стає більш ефективним і виваженим.

УДК 65.012.8 + 004

СЕРГІЙ МИКОЛАЙОВИЧ БОРТНИК
Перший проректор Харківського національного університету внутрішніх справ, доктор юридичних наук, полковник поліції

ПРОБЛЕМИ ПІДГОТОВКИ КАДРІВ ДЛЯ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ УКРАЇНИ

Характерним і незворотним трендом епохи третьої і четвертої промислових революцій є стрімкий перехід матеріальних відносин у віртуальну сферу. Одним з негативних наслідків цього в цілому позитивного процесу є віртуалізація все більшої частки кримінальних правопорушень. Серед фахівців існує думка, що вже в найближчі 10 років зникнуть всі види злочинів, крім кіберзлочинів [1]. І це не популістська заява, а цілком обгрунтоване передбачення, засноване, в першу чергу, на таких двох факторах: а) можливість дистанційного отримання великих коштів незаконним шляхом, і б) відносна безпека і анонімність для виконавця.

Як проміжний етап реагування правоохоронних структур цивілізованого світу на цей виклик є створення підрозділів кіберполіції. В подальшому префікс кібер- можна буде відкинути, оскільки більшість підрозділів поліції будуть займатися профілактикою і розкриттям розгалужених різновидів кіберзлочинів.

Правоохоронці по всьому світу всерйоз готуються до появи підпільних синдикатів, що спеціалізуються на замовних високотехнологічних вбивствах, замаскованих під технічні інциденти різного роду. Беручи до уваги обсяг ринку замовних вбивств в Сполучених Штатах, що становить близько 2 млрд. дол. на рік, фахівці ФБР очікують появу такого мережевого синдикату, а швидше за все не одного, а декількох, в найближчі один-два роки. Враховуючі той факт, що така думка була висловлена 2 роки тому, є підстави вважати, що такий синдикат (синдикати) на поточний момент вже існують.

Головним інструментом подібних синдикатів можуть стати не хакерські програми самі по собі, а штучний інтелект.

Враховуючі вищезазначені обставини, не підлягає сумніву, що для виконання таких злочинів будуть а) залучені висококваліфіковані фахівці в галузі ІТ технологій і інтелектуальної обробки великих масивів даних з відповідно високим матеріальним заохоченням, б) залучене потужне високотехнологічне технічне і програмне забезпечення [1].

З цього незворотно випливає логічний висновок, що кваліфікація фахівців кіберполіції повинна бути як мінімум не гіршою ніж кіберзлочинців. Ситуація ускладнюється тим, що бурхливо розвивається як програмне так і технічне забезпечення комп'ютерів і комп'ютерних мереж, тобто змінюються їх можливості і, відповідно, правила їх застосування, що вимагає від фахівців