структура, штатна чисельність і укомплектованість особового складу підрозділі захисту економіки та слідства Національної поліції України, ефективність їх розстановки, а також стан технічного оснащення вказаних підрозділів не дають можливості забезпечити якісну та своєчасну протидію злочинам у сфері державних закупівель, що негативно впливає на стан оперативної обстановки у цій сфері.

Таким чином можна дійти до висновку, що існуючий стан оперативної обстановки у сфері державних закупівель є досить ускладненим, що вказує на необхідність розробки та впровадження системи заходів, спрямованих на поліпшення стану оперативної обстановки у цій сфері.

Список бібліографічних посилань

1. Бєлкін Л. М. Актуальні проблеми удосконалення законодавства України про державні закупівлі в контексті зниження корупційної складової при їх здійсненні. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 1. С. 81.

2. Шинкаренко І. Р. Моніторинг оперативної обстановки як чинник ефективності протидії злочинності. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2011. Вип. 3. С. 244–255.

3. Плішкін В. М. Теорія управління органами внутрішніх справ : підручник. / за ред. Ю. Ф. Кравченка. Київ : Нац. акад. внутр. справ України, 1999. 702 с.

4. Підготовка інформаційно-аналітичних документів в органах внутрішніх справ України / Підюков П. П., Сущенко В. Д., Лупало О. А., Кондратьєв П. Я., Свірін М. О та ін. ; за заг. ред. Я. Ю. Кондратьєва. Київ : Нац. акад. внутр. справ України, 2005. 87 с.

Одержано 1.11.2018

УДК 342.6

Сергій Васильович ДЕМЕДЮК,
кандидат юридичних наук,
начальник Департаменту кіберполіції Національної поліції України

ДОСВІД РОБОТИ ТА МІЖНАРОДНОЇ СПІВПРАЦІ КІБЕРПОЛІЦІЇ УКРАЇНИ

Департамент кіберполіції було створено в складі Національної поліції України в листопаді 2015 року. Однак, незважаючи на те, що службі лише 3 роки, вже нині векторами та напрацюваннями роботи користуються аналогічні поліцейські підрозділи країн Європи.

Керівництвом нашої держави було поставлено завдання на створення в поліції окремого підрозділу, який був би з одного боку надійним та оперативним комунікатором, як з українськими, так і з міжнародними суб'єктами ринку телекомунікацій (провайдери, ІТ компанії, кластери розробників та програмістів), налагодження взаємодії рівня "Police-Too-Police" та подальший обмін оперативними даними та процесуальними документами з правоохоронцями різних країн світу; а з іншого професійним, високоінтелектуальним поліцейським підрозділом, що виявляє, документує та притягує до відповідальності осіб, що вчиняють кіберзлочини.

За підтримки міжнародних організацій та світових ІТ компаній після створення Департаменту кіберполіції було відразу проведено загальнодержавний набір всіх бажаючих на роботу до кіберполіції на посади спецагентів та поліцейських-оперативників. На одну вакантну посаду було по 400 бажаючих, однак пройшли лише ті – хто відповідав рівням кваліфікації, як технічним так і оперативним. На даний час чисельність підрозділу кіберполіції становить 410 осіб.

Важливо взяти на замітку, що на посади "Спецагентів" нам потрібні "Білі Хакери" – і саме це визначення стало "наживкою" для хакерів вступити до лав поліції і допомагати нині державі та поліції з білого боку.

Структура служби: Департамент кіберполіції складається з головного офісу (HeadOffice), який повністю координує, направляє та контролює роботу; підрозділів програмування та технічного аналізу (Спецагенти), а також практичних підрозділів кіберполіції.

Осередки знаходження наших спецагентів розташовані в 4 ключових місцях нашої держави (Центр, Захід, Південь, Схід) – це розташування допомагає швидко дістатися до осередку кібератаки та знешкодити останній в дуже короткі строки.

Окрім того, саме Спецагенти працюють над створенням різноманітного програмного забезпечення та програмно - апаратних комплексів, яких до речі немає аналогів, що в свою чергу дуже допомагає в оперативному виявленні осіб, які приховуються, як у відкритому, так і прихованому сегменті Інтернет, ідентифікації осіб та предметів, аналізі мереж та системи тощо. До речі, переважна більшість затриманих хакерів до цього часу не розуміє, як ми їх ідентифікували та знайшли – а це саме кропітка робота наших Білих Хакерів. Також, наші Спецагенти орієнтують свою діяльність на виявлення та допомогу в закритті вразливостей на сайтах в органах державної влади, а також державного та приватного сектору.

Спецагенти працюють в постійній взаємодії з кіберполіцейськими-оперативниками, що дозволяє їм обмінюватися думками та вирішувати складні на перший погляд завдання та змінюватися, удосконалюватися і як результат покращувати свої "Soft" вміння.

Оперативні підрозділи кіберполіції розташовані у в кожному територіальному окрузі, а їх в Україні 26, та постійно працюють над виявленням, належним документування злочинної діяльності осіб, їх арешту та притягнення до відповідальності.

Вектор роботи підрозділу є досить широкий, однак основну свою увагу українська кіберполіція звертає саме на протидію кіберзлочинам, а це - виявлення та арешт осіб, які займаються виготовленням, модернізацією, продажем та розповсюдженням різноманітних комп'ютерних вірусів (malware). Ми виявляємо та арештовуємо безліч осіб, які організовують, забезпечують та підтримують Dos та D-Dos атаки на українські та іноземні сегменти, незаконно отримують доступ до техніки та викрадають персональні та білінгові дані, як громадян України, так і інших країн світу; а також незаконно перепродають голосовий трафік.

Окрім того, орієнтуємо наших співробітників на вжиття заходів з припинення злочинів, пов'язаних із незаконним розповсюдженням об'єктів авторського права, що вчиняються через сайти мережі Інтернет та телекомунікаційні мережі та притягуємо до відповідальності осіб, що розповсюджують нелегальний контент. Спрямовуємо роботу на виявлення та арешт осіб, які сексуально експлуатують дітей, виготовляють, розповсюджують та продають дитячу порнографію через відкритий та прихований сегмент Інтернет.

Також, проводимо заходи профілактичного характеру серед населення, щоб останні не стали жертвами шахраїв та не втратили кошти на різноманітних фіктивних фінансових пірамідах та бінарних опціонах. Притягуємо до відповідальності осіб, що вчиняють шахрайські дії через ресурси Інтернет та причетні до злочинів в електронній комерції та незаконного отримання коштів.

Однак, одним з головних напрямків нашої роботи є саме міжнародна взаємодія. Та саме належна поліцейська кооперація та синергія допомагає встановити всіх учасників хакерської злочинної схеми, їх належно задокументувати та, як результат, провести спільні операції з одночасним їх затриманням в різних куточках світу. Наш підрозділ й нині активно приймає участь в великій кількості міжнародних спецоперацій та дуже тісно взаємодіє з усіма підрозділами, емблеми яких розташовані в нижній частині даного слайду.

З даними органами робота налагоджена на рівні "Police-Too-Police", що для лінії "Cyber" є вкрай необхідним, так як хакери знають як затирати та приховувати сліди за собою і без миттєвої кооперації поліцейські нічого не зможуть довести, і, як результат, затримати зловмисника. А тому, робота в рамках міжнародно-правової допомоги, через органи прокуратури та юстиції є вкрай неефективною по нашій лінії, так як в середньому отримання інформації від іншої сторони може зайняти до 3 місяців в найкращому випадку. Для наших справ – це те ж саме що її відразу закрити не починаючи розслідування. Така ж проблематика і в інших країнах світу – а тому ми намагаємося налагодити взаємодію зі всіма поліцейськими колегами, готові ділитися інформацією в оперативному режимі та кооперуватися на напрямку протидії світовим хакерських спільнот.

Так, наразі за участі працівників нашого підрозділу вже проведено 112 міжнародних спецоперацій, у ході яких було арештовано 33 хакери світового рівня та ідентифіковано 8 міжнародних хакерських угрупувань. На території нашої держави було арештовано 5 хакерів,

що вчиняли кіберзлочини (організовували кібератаки, викрадали персональну та білінгову інформацію, паралізували роботу компаній та підприємств), як відносно України так і інших країн світу.

Працівники української кіберполіції приймали активну участь у проведенні міжнародної спецоперації відносно учасників міжнародного хакерського злочинного угрупування, відомого як "Cobalt". До даної групи входили хакери з 5 країн світу, серед яких була й наша країна.

На даний час, установлено що дане хакерське угрупування „Cobalt" причетне до викрадення більш ніж 4 млн. євро. Також встановлено, що їх кібератаки були спрямовані окрім банківського сектору, також і на біржі, страхові компанії, інвестиційні фонди та інші безпосередньо пов'язані з фінансами організації. За результатом проведеної спецоперації, яка проводилася паралельно в Україні, Іспанії, Великобританії, Молдові та Румунії було одночасно затримано та арештовано 5 осіб, що організували та підтримували діяльність даної злочинної групи, а також займалися зняттям коштів з банкоматів.

Досить активно українською кіберполіцією проводиться робота на напрямку виявлення та притягнення осіб, які сексуально експлуатують дітей, виготовляють дитячу порнографію та розповсюджують чи збувають її через ресурси мережі Інтернет.

Досить тісно на даному напрямку нині налагоджена робота з правоохоронними органами Австралії. Обмін інформацією проводиться миттєво, що дозволяє оперативно реагувати та виявляти навіть тих осіб, які приховуються в TORмережах.

Одним з характерних прикладів такої взаємодії є спільна спецоперація України та Австралії, у ході якої було встановлено сімейну пару, яка упродовж останніх двох років сексуально експлуатувала та використовувала свою малолітню доньку, якій було 2 роки для створення порнографічних відеоматеріалів. Продаж відео файлів відбувався в анонімному сегменті всесвітньої мережі Інтернет на більш як десяти тематичних ресурсах. Для анонімізації своїх дій злочинці використовували, як оплату за продаж відео – криптовалюту, а для його розміщення та пропонування – мережу TOR.

Ще одним прикладом належної взаємодії є спільна операція підрозділу ФБР США та працівників кіберполіції України, у ході якої документувалася діяльність злочинної групи, відомої під назвою "FIN7", до якої входило 4 громадян України, які з 2015 року займалися несанкціонованими втручаннями в роботу POS-терміналів світових мереж супермаркетів, готелів розважальних закладів та медичних установ, які належать американським компаніям та компаніям інших країн світу з метою масового викрадення записів із даними кредитних карток громадян Сполучених Штатів Америки, України та інших країн.

Так, зловмисники шляхом розсилки спам-листів, які містять шкідливе програмне забезпечення, працівникам конкретних компаній, отримують віддалений доступ до їх службових комп'ютерів. В подальшому, через внутрішню телекомунікаційну мережу хакери підключаються до серверів процесингових центрів компанії та за допомогою спеціального шкідливого забезпечення, яким інфікують POS-термінали компанії, отримують інформацію про дані банківських карток клієнтів, які скористалися послугами компанії. Викрадена інформація використовується зловмисниками для заволодіння грошовими коштами потерпілих.

Ще одна спільна спецоперація, що проходила під головуванням Європолу, та в ній приймали участь 23 країни світу, яка відома під назвою "Avalanche". У ході проведення даної операції було встановлено 4 особи, які були учасниками хакерського угруповування та особисто розробляли шкідливе програмне забезпечення його постійно модернізували та за допомогою якого здійснювались масові атаки на банківський сектор, міжнародні корпорації та ІТ компанії – інфікували їх серверну та комп'ютерну техніку, після чого здійснювали її блокування, та як результат вимагали грошові кошти за розблокування інформації та надання можливості її нормального використання.

Грошові втрати, пов'язані з кібератаками, проведеними по мережі „Avalanche", за попередніми підрахунками, склали сотні мільйонів євро по всьому світу.

За результатом проведеної спецоперації, яка проводилася паралельно в усіх країнах учасниках, що були залучені до операції було одночасно затримано та арештовано всіх учасників хакерського угруповування. А також заблоковано діяльність всіх доменів, з яких розповсюджувався вірус.

Це лише деякі з тих операцій, що були проведені працівниками підрозділу кіберполіції за час нашого функціонування.

Слід зазначити, що кіберполіція готова працювати в режимі реального часу та надавати інформацію, як для оперативного, так і процесуального використання погодженими каналами зв'язку; наші фахівці готові приймати участь в розробці передового програмного забезпечення необхідного для використання правоохоронцями, а також ділитися уже раніше розробленими програмними продуктами.

Одержано 30.10.2018

УДК 343.435(075)

Тетяна Сергіївна ДЕМЕДЮК,
кандидат юридичних наук,
доцент кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ

ОСОБЛИВОСТІ ДОКУМЕНТУВАННЯ ЗЛОЧИНІВ, УЧИНЕНИХ З МОТИВІВ РАСОВОЇ, НАЦІОНАЛЬНОЇ ЧИ РЕЛІГІЙНОЇ НЕТЕРПИМОСТІ

У Раді Європи вітають прогрес України у боротьбі з ненавистю та дискримінацією, але вказують на наявні проблеми у цій сфері. У п'ятій доповіді про Україну Європейської комісії проти расизму та нетерпимості Ради Європи запропоновано ухвалити нові правові положення щодо розслідування злочинів на ґрунті расової, національної чи релігійної нетерпимості.

За результатами оцінювання звіту України перед Комітетом ООН щодо виконання положень Конвенції ООН про ліквідацію усіх форм расової дискримінації було сформовано зауваження та рекомендації для України, значна частина з яких стосувалися різних аспектів діяльності правоохоронних органів.

Ужиття заходів, спрямованих на усунення негативного впливу етнічної злочинності, радикальних і неформальних молодіжних об'єднань та рухів на оперативну обстановку в державі, підготовка управлінських рішень щодо своєчасного реагування на загострення цієї проблеми та недопущення порушень громадського порядку їх учасниками, є функцією Департаменту карного розшуку Національної поліції України.

Основним недоліком протидії ксенофобії в Україні в ракурсі розслідування злочинів, що вчиняються з мотивів расової, національної чи релігійної нетерпимості, є проблема реєстрації кримінального провадження за відповідними статтями кримінального кодексу України та доказування мотиву злочину.

Кримінальне законодавство України дає певний інструментарій для боротьби із злочинами, вчиненими на ґрунті нетерпимості. Втім, в Україні дотепер зберігається тенденція не кваліфікувати расистські напади як злочини на ґрунті нетерпимості. Навіть тоді, коли є однозначні підстави для кваліфікації злочину як вчиненого на ґрунті ненависті (у тому числі, свідчення підозрюваних), кримінальні провадження порушуються за статтями «хуліганство» або «завдання тілесних ушкоджень».

Аналіз положень кримінального законодавства дозволяє виокремити дві групи злочинів, мотивом вчинення яких є расова, національна чи релігійна нетерпимість.

Перша група – ненасильницькі злочини:

– стаття 161 КК «Порушення рівноправності громадян залежно від їх расової, національної належності або релігійних переконань»;

– стаття 300 КК «Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію»; тощо.

Друга група – насильницькі злочини:

– п. 14 ч. 2 ст. 115 КК «Умисне вбивство» передбачає кваліфікований вид вбивства з мотивів расової, національної чи релігійної нетерпимості;

– ч. 2 ст. 121 КК «Умисне тяжке тілесне ушкодження», передбачає відповідальність