Візуальна оперативна інформація обмежена в своїй здатності розкривати плани і наміри. Як і радіотехнічну оперативну інформацію, візуальну оперативну інформацію дорого збирати, а обсяги даних, що генеруються, роблять управління такою інформацією важким процесом. Окрім того, візуальна розвідка також вразлива для заходів з недопущення та дезінформації.

Джерела пов'язані з розвідкою фізичних полів (**Measurement and Signatures Intelligence**) Розвідка фізичних полів (MASINT) є новітньою формою збору даних та включає в себе дані про випромінювання, наприклад, теплове і звукове, та дані про залишки речовин, на кшталт відбитків пальців, слідів, зразків тощо. Розвідка фізичних полів (MASINT) має перевагу, тому що цілі часто не усвідомлюють можливостей цього методу збору даних.

Для ефективного проведення боротьби з кіберзлочинністю працівники поліції, застосовуючи інструментарій аналітичної діяльності, повинні враховувати можливості та об'єктивні обмеження, що виникають під час розвідки у відкритих джерелах (**Open Source Intelligence**) та джерелах таємної інформації (**Human Source Intelligence**).

Одержано 18.04.2016

*

УДК 004.056:55(043.2)

Олена Русланівна Лапшина,
курсант 3 курсу факультету № 4 ХНУВС
Науковий керівник: канд. техн. наук Світличний В. А.

ПРОТИДІЯ ФІШИНГ-ШАХРАЙСТВУ

На сьогоднішній день постійно використовується безліч різних високотехнологічних пристроїв – пластикових карт, мобільних телефонів, комп'ютерів. Постійно з'являються нові моделі, програми і сервіси. Все це робить наше життя зручнішим, але потребує деяких навиків і знань.

Одночасно з розвитком таких пристроїв з'являються види шахрайства, які дозволяють присвоїти грошові кошти громадян. Щоб не піддатись на прийоми зловмисників, достатньо знати, як вони діють, і отримуватись правил безпечного використання.

Аналітичні дослідження дозволяють стверджувати, що найбільш розповсюдженим шахрайством являється шахрайство з банківськими картами. Простота використання банківських карт залишає безліч лазівок для шахраїв.

Розглянемо найпопулярніший спосіб шахрайства з картами банків:

Як це організовано? Ви отримали лист по електронній пошті (в тому числі із банка), Вам зателефонували з банка, Вам приходить SMS повідомлення, або про те, що Ваша банківська карта заблокована і для її розблокування пропонується:

– зайти на сайт банка і особисто розблокувати карту. Не переходьте по вказаним в листі посиланням, оскільки вони можуть привести на фальшиві сайти-двійники;

– безкоштовно зателефонувати на певний номер для отримання подробиць інформації. Коли ви дзвоните на вказаний телефон, вам повідомляють про те, що на сервері, який відповідає за обслуговування карти, виник збій, а після того просять повідомити номер карти і ПІН-код для її перереєстрації.

Насправді відбувається наступне: для шахрайства зловмисникам потрібен тільки номер Вашої карти і ПІН-код. Як тільки Ви їх повідомите, кошти будуть зняті з Вашого рахунку. Як діяти в такій ситуації? Не поспішайте повідомляти реквізити вашої карти! Ні одна організація, включаючи банк, не може вимагати Ваш ПІН-код! Для того, щоб перевірити отриману інформацію про заблокування карти, необхідно зате-

лефонувати в службу підтримки банка. Скоріше всього. Вам дадуть відповідь, що ніяких збоїв на сервері не було, і Ваша карта продовжує обслуговуватись банком.

Протидія фішингу потребує постійного моніторингу на предмет нових методів та шляхів обходу системи безпеки в цілому, але дані в основному потрапляють до рук шахраїв через «людський фактор». адже більша частина населення не придає особливого значення звичайним правилам особистої безпеки. Тому шахраї, використовуючи методи соціальної інженерії, мають можливість заволодіти особистими даними людини, які вона мала необережність розкрити.

Одержано 28.04.2016

УДК 004.042

Дмитро Васильович Мільчаков,
курсант 3 курсу факультету № 4 ХНУВС
Науковий керівник: канд. техн. наук Світличний В. А.

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС АНАЛІТИЧНОГО СУПРОВОДУ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ Й ПІДТРИМКИ УХВАЛЕННЯ РІШЕНЬ – RICAS

Фахівцями Управління інформаційного забезпечення Харківського обласного ГУНП спільно з місцевими ІТ-компаніями розроблений інноваційний комплекс аналітичної обробки інформації різноманітних банків даних з відображенням на детальній інтерактивній карті як самих об'єктів, так і результатів їх аналізу. Комплекс має робочу назву «RICAS» (Real – time Intelligence Crime Analytics System) і на сьогоднішній день знаходиться на етапі тестового впровадження.

Застосування комплексу дає можливість:

- збереження відеоданих на серверах, їх перегляд та аналіз у разі необхідності;
- безпосереднього доступу до кожної відеокамери на детальній інтерактивній карті області;
- відображення на цій карті об'єктів та осіб, які можуть впливати на розвиток ситуації.

В процесі тестування комплексу підтверджується його гнучкість та спроможність інтегрування будь-яких даних, з можливістю часового та просторового аналізу їх зв'язків між собою. Розроблений комплекс не обмежується Харковом та областю, а з легкістю масштабується до рівня країни і навіть більше.

Однією із складових частин комплексу RICAS є зовнішній Інтернет – сервіс взаємодії правоохоронних органів з громадськістю – проект Police.kh.ua, який на даний час користується популярністю в мережі Інтернет.

Проведені тестові випробування впродовж 3-х місяців підтверджують можливості комплексу щодо реагування на кримінальні та інші події. В результаті роботи команди з 3 аналітиків протягом цього часу було надано 152 аналітичних довідки з відомостями про осіб, можливо причетних до вчинення злочинів, більшу половину з яких підтверджено в ході перевірочних та оперативних заходів, зазначених осіб викрито у вчиненні злочинів.

На теперішній час комплекс тестується на обчислювальних потужностях ГУНП в Харківській області. Для його розгортання в робочий режим необхідне створення сучасного дата-центру на базі ГУНП в Харківській області, створення ситуаційно-аналітичного центру та організація підготовки відповідних фахівців для роботи в ньому.

Комплекс RICAS працює в реальному часі і дозволяє розкривати злочини на основі аналізу баз даних, накопичених поліцією/міліцією за останні 20 років. Системі доступні дані про більш ніж 5 мільйонів подій, що сталися на Харкі-