які на законодавчому рівні визнали торгівлю людьми тяжким злочином.

Список використаних джерел:

1. Палажій Г. В Україні почастішали випадки торгівлі людьми та рабства. Як не стати жертвою? URL: http://zik.ua/news/2017/03/28/v_ukraini_pochastishaly_vypadky_torgivli_lyudmy_ta_rabstva_yak_ne_staty_1069197 (дата звернення: 13.10.2017).
2. Биткойн - это инновационная сеть платежей и новый вид денег! URL: https://bitcoin.org/ru/ (дата звернення: 15.10.2017).
3. Торгівля людьми в Україні. Актуальні ризики та вразливі групи. URL: http://pidmoga.info/torgivlya-lyud-my-v-ukrayini-aktual-ni-ry-zy-ky-ta-vrazly-vi-grupy/ (дата звернення: 15.10.2017).
4. Кримінальний кодекс України: закон України від 05.04.2001 № 2341-III. URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 08.10.2017).

Одержано 30.10.2017

УДК 004.056.57

Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук, доцент кафедри кібербезпеки факультету №4 Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Інформаційний простір давно став безпосередньою і невід'ємною частиною нашого життя, але незважаючи на усі заходи, що приймають окремі особи, установи, держава, кіберзлочинність продовжує свою діяльність. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців. Будь-який зловмисник перш за все – людина, отже має певні вразливості психіки, які можливо використовувати при проведенні розслідування. В залежності від психологічних особливостей кіберзлочинця, можливо виділити певні вразливості його психіки та ефективно впливати методами і прийомами соціальної інженерії на нього.

Кіберзлочинець, який скоїв злочин, розуміє, що він порушив закон, тому в більшості випадків не виключено, що на підсвідомому рівні він боїться свого викриття, тому він більшу частину часу перебуває в страху. Це призводить до втрати

уваги та сконцентрованості, що, при правильному застосуванні техніки соціального інжинірингу, можливо використати на користь оперативного працівника, який розслідує даний злочин. Беручи до уваги той факт, що більшість кібезлочинів здійснюються з метою самоствердження, то цілком природно буде вважати, що такого кіберзлочинця будуть обурювати почуття марнославства та бажання того, що б про його діяння стало відомо щонайбільшій кількості людей. Така поведінка дуже розповсюджена серед молодих та недосвідчених представників хакерської спільноти, особливо серед тих, хто до цього не зіткався з представниками кіберполіції і не потрапляв у ситуації, коли до нього застосовується судове переслідування. В такому випадку правильно організований пошук інформації в мережі Інтернет може допомогти при встановленні особи порушника або пошуку його реквізитів, таких, як IP і MAC адреси, або контактні дані для ведення листування. У ході листування можливе застосування технік соціального інжинірингу з метою отримання інформації щодо причетності особи до вчинення певного злочину. Також для можливості стеження за кіберзлочинами, що скоєні або плануються, працівник поліції може впроваджуватися в спільноти хакерів під виглядом такого ж хакера з метою отримання довіри до себе. В результаті такий працівник може мати доступ до найсвіжішої та актуальної інформації щодо кібезлочинів, які скоюються цією спільнотою з наступною реалізацією цієї інформації, розслідування кібезлочинів, пошуку та відстеження контактних даних та реальних імен та адрес хакерів, притягнення їх до відповідальності за вчинені злочини. Така методика може мати характер інсайдерінгу в цілях недопущення та попередження кіберзлочинів. При впровадженні працівника в хакерську спільноту для розслідування кіберзлочинів, він може для встановлення особи зловмисника, застосовувати прийом провокації та дезінформації. Крім того для ефективного розслідування або недопущення кіберзлочінів цілком обґрунтовано використання метода «подвійній агент». Як відомо, подвійним агентом називається особа, яка одночасно співпрацює з двома різними організаціями (службами, спільнотами), які, зазвичай, протиборствують. Подвійний агент, який систематично веде роботу в осередку злочинців та направляє їм різного роду дезінформацію, проводить провокаційну діяльність під легендою – прикриттям, тобто здійснює оперативну гру. Подвійних аге-

нтів можливо розділити за декількома категоріями в залежності від особливостей їх роботи:

- «торговець» – агент, який доставляє інформацію одній стороні в обмінна отримання інформації про другу сторону;
- «кріт» – працівник однієї сторони, який потайки співпрацює з другою;
- «лжекріт» – працівник однієї сторони, який за завданням свого керівництва пропонує свої послуги другій стороні або дозволяє себе завербувати;
- «перевертень» – працівник однієї сторони, якого було розкрито і який погодився на співпрацю з іншою з метою уникнення покарання або іншою.

Природно, що методи соціального інжинірингу для розслідування кіберзлочинів можуть застосовуватись кіберполіцією у всіх випадках та порядку, коли вони відповідають вимогам чинного законодавства, діючих підзаконних актів та міжнародних законодавчим документам. Здійснивши аналіз вразливості людської психіки, можливо виявити вразливості кіберзлочинця та можливості використання їх для розслідування кіберзлочинів. На основі цих вразливостей слід взяти до уваги інші базові методи соціального інжинірингу, які потрібно застосовувати для розслідування кіберзлочинів, а саме:

- використання бренда відомої корпорації;
- підроблена лотерея;
- фальшиві антивіруси і програми для забезпечення безпеки (scareware);
- фішинг і його різновиди;
- фрікінг;
- претекстінг;
- quid pro quo;
- «дорожнє яблуко»;
- збір інформації з відкритих джерел головним чином з соціальних мереж;
- плечовий серфінг (shoulder surfing);
- зворотна соціальна інженерія.

Крім того, на нашу думку, працівник кіберполіції може для розслідування кіберзлочинів використовувати спільно з методами соціального інжинірингу відомі методи оперативно-розшукової діяльності, але інтерпретовані під використання в кіберпросторі.

Одержано 25.10.2017