

процесів, зокрема їх кримінально-правового аспекту. Це обумовило наявність у чинному Кримінальному кодексі (далі – КК) ст. 359, що встановлює кримінальну відповідальність за незаконне поводження із СТЗНОІ. Попри той факт, що перші згадки про кримінальну відповідальність за злочини у сфері незаконного використання СТЗНОІ з'явилися у вітчизняній кримінально-правовій доктрині, а потім й у кримінальному законодавстві ще до ухвалення КК 2001 р., в Україні досі існує значна кількість проблем, пов'язаних з кримінальними посяганнями, в яких використовуються СТЗНОІ.

З урахуванням сучасного стану розвитку інформаційно-комунікаційних технологій, протягом трьох років з моменту набрання чинності 07.07.2010 р. Законом України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне поводження зі спеціальними технічними засобами негласного отримання інформації» від 15.06.2010 року № 2338-VI, в Україні спостерігається тенденція до збільшення випадків притягнення осіб до кримінальної відповідальності за вчинення злочину, передбаченого статтею 359 КК України.

Відповідно до цього закону, поряд з відповідальністю за незаконне використання спеціальних технічних засобів негласного отримання інформації (далі – СТЗ) було встановлено відповідальність за незаконне придбання та збут таких засобів (зміни у статті 359 КК України). Так, згідно інформації Служби безпеки України – порушено кримінальних справ (проваджень) за статтею 359 КК України: у 2010 році – 20, у 2011 році – 114, у 2012 році – 148, за період з січня – квітня 2013 року – 185.

Крім того, за даними Єдиного державного реєстру судових справ за цією ж статтею у 2018 році було порушено 108 справ, у 2017 році – 137, у 2016 році – 153, у 2015 році – 99.

Отже, належний захист прав людини від злочинних посягань в рамках використання, придбання та збуту СТЗНОІ потребує більшої уваги з боку законодавця, так як захист фундаментальних прав, на рівні з іншими, є одним з основних завдань держав ЄС і має стати пріоритетним завданням для України.

Одержано 17.04.2019



УДК 004.58/316.776

Роман Олексійович БОДНАР,

курсант групи Ф4-102 ХНУВС

Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

СОЦІАЛЬНА ІНЖЕНЕРІЯ, ЩО ВИКОРИСТОВУЄТЬСЯ ШАХРАЯМИ

Соціальна інженерія – це метод отримання необхідного допуску до інформації, заснований на особливостях психології людей. Основною метою соціальної інженерії є отримання доступу до конфіденційної інформації, паролів, банківських даних і інших захищених систем. Відомо, що найбільш

слабка ланка в системі забезпечення інформаційної безпеки – це людина. Чому люди вразливі для атак?

- 1) Ну перш за все, через банальну втрату пильності.
- 2) Дуже легко вірять отриманій інформації, не залежно від її джерела розповсюдження.
- 3) Вважають політику інформаційної безпеки лише марною тратою сил та часу.
- 4) Щиро хочуть допомогти кожному, хто попросить по допомогу.
- 5) Не усвідомлюють шкідливих наслідків своїй дій.
- 6) Недооцінюють важливість інформації якою володіють.

Засоби, які використовуються шахраями, найбільш часто і успішно використовуються в спробах маніпулювати людьми:

Авторитетність. Злодій отримає потрібну відповідь, якщо людина впевнена, що людина яка запитує має право і владу задавати це питання.

Взаємність. Роз'яснювати тут багато не має сенсу, коли хтось робить щось для нас, ми відчуваємо бажання віддячити взаємністю.

Відповідальність. Люди мають звичку виконувати обіцянки, пообіцяв, ми зробимо все щоб не показатися не заслуговуючими довіри, а також багато інших.

Методи соціальної інженерії:

Претекстінг (Pretexting) – це набір дій, проведених по характерному, спланованому сценарію, в результаті якого людина може видати будь-яку інформацію або здійснити якусь характерну дію.

Фішинг (password harvesting fishing) – отримання необхідних злочинцю даних за допомогою сервісів миттєвих та смс повідомлень.

«Троянський конь» – шкідлива програма, яка використовується для збирання, винищення або модифікації інформації, порушення роботи комп'ютера або використання ресурсів користувача в своїх цілях.

«Кви про кво» – метод соціальної інженерії, який використовується шахраями з метою заповучення інформації в обмін на допомогу користувачеві.

Найбільш банальний, але й найбільш небезпечніших метод «Подсматривание через плечо» – метод включає в себе спостереження за особистою інформацією користувача через його плече.

Звичайно були приведені лише найбільш поширені методи соціальної інженерії, яка може використовуватися шахраями, та більш за того, ці методи з'являються все більше і більше з кожним днем.

У якості висновку слід зазначити, що основним недоліком у сфері запобігання негативним проявам соціальної інженерії є відсутність системної роботи щодо її виявлення та подолання, наявність лише декларативних положень у стратегіях та відсутність прийнятих законодавчих та підзаконних актів на їх конкретизацію та розвиток, низький рівень інформованості населення щодо можливих загроз соціальної інженерії, а також високу латентність злочинів у цій сфері, що унеможлиблює виявлення та притягнення до відповідальності усіх винних осіб.

Одержано 22.04.2019

