Тарасенко О.С.
кандидат юридичних наук,
доцент кафедри оперативно-розшукової
діяльності Національної академії
внутрішніх справ

ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК ЗАСІБ ПОПЕРЕДЖЕННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

XX століття подарувало людству нові форми отримання, передачі та опрацювання інформації. При цьому, щодня удосконалюються та розвиваються різноманітні інформаційні ресурси, комунікатори зв'язку, загалом комп'ютерні технологій та мережа Інтернет.

На сьогодні достатньо мати смартфон, з під'єднанням до мережі Інтернет, для того щоб можна було здійснити оплату в магазині, замовити доставку товару, відправити та отримати електронну пошту, отримати інформацію з Інтернет ресурсів, спілкуватися за допомогою соціальних сторінок, в тому числі у форматі відео конференції, навіть ставити цифровий підпис.

На перший погляд всі ці аспекти спрощують та покращують існування громадян, утім, не секрет, що користуючись персональним комп'ютером (стаціонарним, портативним, планшетним), смартфоном тощо – особа піддається певним ризикам щодо захисту своїх даних, які можуть використовуватися з метою вчинення злочину та в корисливих цілях іншими особами. Здебільшого ці злочини пов'язані із викраденням особистих даних особи, даних кредитних карток, відомості про особисте життя, інформація щодо роботи установи тощо. Отже, отримуючи доступ до особистих даних особи, можна не лише викрасти кошти, які знаходяться на рахунках, а й приймати розпорядчі рішення, подавати відомості до державних установ тощо.

Необхідно зазначити, що трапляються випадки, що громадяни інколи самі «халатно» відносяться до захисту своїх даних, ти м самим спрощують

доступ них сторонніх осіб. Здебільшого це зводиться до відсутності на комп'ютері, комунікаторі різноманітних «антивірусних» програм, наявність проблем у роботі відповідного пристрою, порушення в роботі електронної пошти чи соціальної сторінки, наявність листів на електронній пошті із підозрілим змістом тощо.

У той же час, зволікання користувача на певні проблеми в роботі персонального комп'ютера (стаціонарного, портативного, планшетного), смартфона тощо призводить до втрати дорогоцінного часу своєчасного виявлення осіб, які несанкціоновано втручаються у відповідний пристрій (засіб) та отримують необхідні відомості.

Отже, своєчасне виявлення шкідливого програмного забезпечення надасть можливість попередити незаконне викрадення даних особи (особисті дані, дані кредитних карток, відомості про особисте життя тощо), припинити загалом несанкціоноване втручання в роботу інформаційної системи та виявити осіб причетних до такого втручання.