кооперативна гра тощо).

4) застосування класичного теоретико-ігрового аналізу до поставленої задачі.

Неконтрольований вплив гравців з деструктивними цілями на користувачів соціальної мережі може призвести до виникнення загроз інформаційній безпеці окремої особистості, спільноти або держави.

Інша задача динамічного аналізу – прогнозування формування зв'язків. Дана задача полягає у визначенні, чи будуть дві конкретні вершини з'єднані одна з одною через деякий проміжок часу. Для її вирішення застосовують автоматичне моделювання процесу розвитку соціальної мережі з використанням таких характеристик мережі як кількість спільних сусідів, геодезична відстань, впливовість вершин тощо.

З погляду інформаційної безпеки держави, динамічні методи аналізу соціальних мереж корисні тим, що дозволяють прогнозувати формування та динаміку поглядів акторів під час інформаційно-психологічних впливів та інформаційно-психологічного керування.

Література:

1. Строк Ф.В. Консенсус в социальных сетях: динамический подход / Ф.В. Строк // Доклады Всероссийской научной конференции «Анализ изображений, сетей и текстов» – АИСТ'2012. Екатеринбург, 16-18 марта 2012 г. – С. 264–272.

2. Губанов Д.А. Социальные сети: модели информационного влияния, управления и противоборства. / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили. – М.: Физматлит, 2010.

3. Батура Т.В. Методы анализа компьютерных социальных сетей / Т.В. Батура // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2012. – Т. 10, № 4. – С. 13–28.

4. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

5. DavernM.Social Networks and Economic Sociology: A Proposed Research Agenda for a More Complete Social Science / M. Davern // The American Journal of Economics and Sociology. – 1997. – Vol. 56, No. 3. – P. 287-302.

6. Hanneman R. A. Introduction to Social Network Methods (free introductory textbook on social network analysis). / R. A. Hanneman, M.D. Riddle – 2005. [Електронний ресурс] Режим доступу: http://faculty.ucr.edu/~hanneman/

Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Миколенко О.М.
кандидат юридичних наук, доцент,
доцент кафедри кримінального права, кримінального процесу та криміналістики
Одеського національного університету імені І.І. Мечникова

Розвиток сучасних інформаційних технологій, удосконалення виробництва і розширення сфери застосування новітньої кібернетичної техніки дали можливість зародження специфічного, складного виду злочинних діянь, де комп'ютерне оснащення та електронна інформація є об'єктом протиправного посягання. Поряд з позитивними здобутками, інформатизація супроводжується побічним, негативним явищем криміногенного характеру, до якого відносять злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

На сучасному етапі технологізації суспільства: обробки та обміну інформацією за допомогою міжнародної глобальної мережі INTERNET, відбуваються негативні процеси – перехід від простої поодинокої комп'ютерної злочинності до організованої – складної. На жаль, спостерігається динаміка злиття новоявленої злочинності з міжнародним криміналітетом, що несе у собі відповідну загрозу суспільству в цілому. Слід зазначити, що така транскордонність ускладнює можливості розкриття та розслідування цієї категорії злочинів працівниками правоохоронних органів різних держав.

До переліку негативних чинників розповсюдження цієї категорії злочинів та низького рівня їх розкриття можна віднести:

1. Низький рівень контролю за тиражуванням та розповсюдженням програмної комп'ютерної продукції.

2. Високу латентність злочинів. Лише 10 – 15 % комп'ютерних злочинів стають відомими правоохоронним органам**.**

3. Недостатність теоретичних знань і практичних навичок розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, інформаційних технологій практичними працівниками правоохоронних органів, неможливість доведення до суду кримінальних проваджень цієї категорії.

Зупинимо свою увагу саме на останньому чиннику. Слід зазначити, що досудове розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та збирання доказів по цим справам, істотно відрізняються від розслідувань інших "традиційних" злочинів, або зазвичай буває більш складним. За цими кримінальними справами найчастіше допускаються помилки, що пояснюється відсутністю належного рівня теоретичної та практичної підготовки оперативних працівників і слідчих. Таке розслідування не вимагає спеціальної технічної підготовки слідчого або прокурора, і в більшості випадків залежить від грамотної та досвідченої роботи експертів.

Результати аналізу практичної діяльності правоохоронних органів по розслідуванню злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку свідчать про те, що дослідження комп'ютерної техніки доцільно проводити в умовах криміналістичної лабораторії, де цю роботу виконують фахівці з необхідною професійною підготовкою. Адже докази, що пов'язані з комп'ютерними злочинами, які були вилучені з місця події, можуть бути легко змінені, як в результаті помилок при їх вилученні, так і в процесі самого дослідження [1, с. 81-85]. Таким чином, незважаючи на де-юре, відсутність законодавчої вимоги про обов'язкове призначення експертизи в цих провадженнях, де-факто, без призначення і проведення експертизи не можна говорити про ефективне розслідування таких справ.

Також окремою проблемою є процес представлення доказів в судовому процесі, який вимагає спеціальних знань і відповідної підготовки. Тут не можна недооцінювати роль експертизи, яка може дати кваліфіковану відповідь на поставлені питання. Однак експертиза вимагає якогось часу не тільки на її проведення, а й на пошук відповідних фахівців, а при вилученні комп'ютерної техніки часто важливим фактором, що дозволяє зберегти необхідну доказову інформацію, є раптовість та оперативність. Саме тому вилучення комп'ютерів і інформації доводиться проводити тими силами, які є в наявності, тобто слідчими або оперативними підрозділами. І в цьому випадку саме слідчий не застрахований від помилок, обумовлених недостатністю знань, що пізніше використовується захистом в суді.

Отже, поставлена проблема має два аспекти: загальні помилки, які допускаються працівниками правоохоронних органів при розслідуванні комп'ютерних злочинів, і технічні аспекти, пов'язані із захистом інформації, яка встановлюється на комп'ютерах їх безпосередніми користувачами.

Не менш складною є і робота прокурора у суді: обвинувачення у справах по комп'ютерним злочинам має будуватися так, щоб судді, присяжні та сторони провадження, які мало знаються на комп'ютерах і комп'ютерних програмах, змогли зрозуміти складні технічні моменти та процеси, дослідити докази по справі. Слабкі знання специфіки технічних проблем суддею або присяжними можуть бути навіть небезпечними для кримінального провадження. Як приклад, можна навести судовий розгляд відомої справи Роберта Т. Моріса про запровадження ним програми-хробака (вірус Моріса) до мережі Інтернет у 1988 року [2]. Вірус Моріса інфікував 6 200 комп'ютерів. І незважаючи на те, що ця програма не завдала прямих матеріальних збитків (не були викрадені чи пошкоджені дані), комп'ютерні центри і звичайні користувачі зазнали збитків за час виявлення цієї програми і час, який був потрібен на перевірку та відновлення працездатності системи. Під час обвинувального процесу, обвинувачуваний підтвердив впровадження програми-хробака, але заявив, що це було зроблено необережно. У результаті Роберта Т. Моріса було засуджено умовно. І таких випадків, коли умовне засудження назначалося за комп'ютерні злочини, які принесли багатомільйонні збитки, чимало.

Отже, підводячи підсумок, наполягаємо на обов'язковій участі спеціаліста при провадженні слідчих (розшукових) дій при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Крім того, вважаємо за необхідне постійну участь фахівця у стадіях судового провадження та здійснення ним, так би мовити, технічного "супроводу" кримінального провадження, адже слабкі знання специфіки технічних проблем суддею або присяжними можуть нашкодити провадженню, зокрема, зрадлива інтерпретація доказів може призвести до хибного висновку, і як результат - неправосудного судового рішення.

Література:

1. Моїсеєв О.М. Залучення спеціаліста до розслідування комп'ютерних злочинів / О.М. Моїсеєв // Правові основи захисту комп'ютерної інформації від протиправних посягань: Матеріали міжвузівської науково-практичної конференції (м. Донецьк, 22 грудня 2000 р.). – Донецький інститут внутрішніх справ, 2001. – С. 81 – 85.
2. Атака на INTERNET [Електронний ресурс]. – Режим доступу: http://www.sources.ru/security/attack2/09-04.html. – Назва з екрану.

Перспективы использования пористого кремния в качестве датчиков систем с контролем доступа

Мирошниченко А.І.
преподаватель ассистент
кафедры общетехнической и фундаментальной подготовки
Одесской государственной академии технического регулирования и качества

Лещенко О.І.
доцент кафедры компьютерных и информационно
измерительных технологий
Одесской государственной академии технического регулирования и качества

С ростом современных технологий все более остро стоит вопрос защиты, как персональных данных, так и защиты оборудования от несанкционированного вскрытия и доступа. Помимо защиты с помощью специальных программ, которые имеют возможность блокировать и, или, фиксировать несанкционированные доступы в систему, используются также разнообразные датчики. Основное требование к таким датчикам – это дешевизна (особенно если они одноразового использования), простота в изготовлении, широкий спектр электрических и люминесцентных свойств. Наиболее пригодным материалом для этих целей может быть пористый кремний, который представляет собой сложную структуру нанокристаллитов.

Пористый кремний изготавливается путем анодного травления монокристаллического в растворах плавиковой кислоты. Одно из достоинств этого материала является то, что свойства получаемого в результате образца сильно зависят от многочисленных факторов – кристаллографического направления подложки, уровня легирования, а также типа легирования, концентрации плавиковой кислоты, плотности тока анодирования, времени травления, последующей термообработке, уровня освещенности во время травления. Управляя этими факторами можно получить образец с заданными параметрами, наиболее подходящими для решения поставленной задачи. Однако, несмотря на многочисленные опыты, до сих пор нет полной картины образования пористого кремния. В частности, мало исследованы свойства пористого кремния, изготовленного на подложках с кристаллографической ориентацией (110). Эти исследования необходимы, так, как получив полную картину образования данного материла, и, научившись управлять процессом изготовления, можно получить в распоряжение дешевые датчики, имеющие широкий спектр применения.

Исследовались фотолюминесцентные свойства пористого кремния, полученного на подложке на подложках КДБ-10, с удельным сопротивлением 10 Ом·см, с кристаллографической ориентацией (110). Травление производилось в растворе плавиковой кислоты, в ячейке с горизонтальным расположением электродов, где анодом служила платиновая сетка, а катодом – поверхность самой пластины кремния. В качестве переменного параметра было выбрано время травления, которое изменялось от 5 до 30 минут. Фотолюминесценция возбуждалась газовым лазером с длиной волны 330 нм, средней излучательной мощностью около 3 мВт, длительностью импульса 10 нс. Спектры записывались непосредственно на компьютер с помощью специальной программы. Результаты представлены на рисунке 1.