Система ставить з ніг на голову традиційну банківську таємницю: всі операції проводяться відкрито, але пов'язати конкретну адресу з конкретною людиною не являється можливим.

*Одержано 17.04.2018*

УДК 004.056.53:351.74

**Павло Ігорович ДРАГУНОВ,**
курсант групи Ф4-102 ХНУВС
*Науковий керівник: завідувач кафедри кібербезпеки*
*факультету № 4 ХНУВС кандидат технічних наук, доцент Гнусов Ю. В.*

## ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ З ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З метою протидії злочинності, ефективного попередження, припинення та розкриття злочинів органи та підрозділи Національної поліції України здійснюють необхідні: слідчі (розшукові) дії; негласні слідчі (розшукові) дії; оперативно-розшукові дії. Під час підготовки та проведення зазначених дій працівники поліції використовують інформацію з обмеженим доступом в акустичному та електронному вигляді.

Така інформація може циркулювати в акустичному вигляді під час проведення нарад щодо планування певних негласних заходів. В електронному вигляді інформація циркулює, наприклад, під час підготовки необхідних документів, таких як плани, звіти, клопотання до суду.

Дана інформація може бути цікавою для представників організованих злочинних груп, та, навіть, представників іноземних розвідок. Вони можуть отримати доступ до цієї інформації шляхом фізичного доступу на об'єкт де циркулює ця інформація (в службовому кабінеті працівника поліції).

Також за допомогою сучасних приладів зловмисники можуть аналізувати бездротові мережі (Wi-Fi) та вилучати незаконним методом данні жертви. Сучасні засоби технічної розвідки дозволяються підключатися дистанційно до обчислювальних машин, створювати перешкоди у телекомунікаційних каналах між пристроями і супутниковою системою, бездротових мережах.

В разі отримання несанкціонованого доступу сторонніх осіб до інформації з обмеженим доступом, це може призвести до більш ефективної протидії злочинців щодо документування їх діяльності з боку працівників правоохоронних органів або неможливості затримання злочинців.

З метою не допущення витоку інформації з об'єктів інформаційної діяльності поліції необхідно вживати заходів з технічного захисту інформації, таких як періодичний пошук засобів негласного зйому інформації («закладних пристроїв») та використання технічних засобів захисту акустичної інформації та електронно-обчислювальних машин.

На сьогоднішній день на ринку представлено багато різних за призначенням та технічними можливостями технічних засобів пошуку та захисту інформації, як українського так і закордонного виробництва. При цьому періодично на ринку з'являються нові розробки та нові технічні засоби.

Під час вибору технічних засобів, що будуть використовуватися для забезпечення захисту інформації, слід звернути увагу на такі технічні засоби як:

1. Тепловізори – використовуються для виявлення пристроїв, що виділяють температурне поле. Зазвичай ці прилади приховуються зловмисником у стінах.

2. Багатофункціональні пошуковий прилади – зазвичай вони поєднують в собі широкосмуговий детектор електромагнітного поля, приймач інфрачервоного діапазону, різні додаткові зонди для перевірки провідних ліній і оцінки віброакустичного захисту приміщення.

3. Частотоміри – дозволяють виміряти частоту сигналу безконтактно, за допомогою антени. Така властивість дозволяє застосовувати їх як для замірів «відомих» сигналів, так і для пошуку «прихованих» сигналів від підслуховуючих пристроїв (жучків).

Таким чином, можна зробити висновок, що для забезпечення захисту інформації з обмеженим доступом від витоку з об'єктів інформаційної діяльності Національної поліції можуть використовуватися різноманітні технічні засоби, як пошукові та засоби захисту інформації.

*Одержано 17.04.2018*

УДК 004.159.9

**Ярослав Віталійович ОСІПОВ,**
курсант групи Ф4-202 ХНУВС
*Науковий керівник: викладач кафедри кібербезпеки*
*факультету № 4 ХНУВС кандидат технічних наук Світличний В. А.*

## СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК СПОСІБ ШАХРАЙСТВА

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

Є декілька головних векторів нападу, які використовуються при проведенні атак за допомогою соціальної інженерії:

– Он-лайн;

– Телефон;
– Аналіз сміття;
– Особисті підходи;

Однак крім цього, ви також повинні знати цілі нападу, розуміти, що хакер сподівається отримати. Його цілі засновані на тих же потребах, які керують усіма нами: гроші, соціальний поступ і самоствердження.

***Мережеві (он-лайн) загрози:*** У нашому все більш і більш пов'язаному діловому світі, персонал часто використовує інформацію і відповідає на запити, які отримує за допомогою електроніки з середини і зовні компанії. Таке забезпечення зв'язку дає можливість хакерам підійти до вашого персоналу, використовуючи відносну анонімність Internet.

***Аналіз сміття:*** Незаконний аналіз сміття – цінна діяльність для хакерів. Ділові паперові відходи можуть містити інформацію, яка має безпосередню вигоду для хакера (наприклад номера рахунків і призначених для користувача ідентифікаторів) або можуть служити основною інформацією, наприклад, телефонний довіднико-організації або списки співробітників.

***Особистісні підходи:*** Для хакера найпростіший і найдешевший шлях отримання інформації – це попросити про це безпосередньо. Цей підхід може здаватися грубим і очевидним, але це основа шахрайства з незапам'ятних часів. Існує чотири різновиди такого підходу:

– Залякування.
– Переконання.

***Фізичні підходи:*** Менш поширений, але більш ефективний для хакера підхід є прямим, особистим контактом з адресатом. Хоча ці підходи мають набагато більші ризики для злочинця. Зростання в використанні мобільних технологій, які дають можливість користувачам приєднатися до корпоративних мереж, в той час як вони знаходяться в дорозі або вдома, є іншою головною загрозою IT-ресурсі в компанії. Можливі напади включають як найпростіші нападу, так і більш складні. Хоча основна частина великих компаній розробила інфраструктури захисту сайту, однак, офіси середнього розміру можуть бути слабкіше обізнані про правила контролю відвідувачів офісу. Ситуація, в якій злочинець слід за кимось, проходячи в офіс, є дуже простим прикладом нападу з використанням соціальної інженерії. Правила повинні передбачати неможливість проходу в будівлю компанії без належного дозволу.

Отже, захист від атак соціальної інженерії безсумнівно, одне з найскладніших в розробці справ. Даний тип захисту не можна побудувати виключно технічними методами. Крім того, хотілося б відзначити що для побудови системи протидії таким атакам, безсумнівно, варто залучати професійних консультантів, а не намагатися будувати захист своїми силами.

*Одержано 17.04.2018*

## *НАУКОВИЙ ГУРТОК КАФЕДРИ КАФЕДРИ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ТА РОЗКРИТТЯ ЗЛОЧИНІВ ФАКУЛЬТЕТУ № 2*

УДК 35.078:342.738

**Віталій Олегович НАЙДА,**
курсант групи Ф1-203 ХНУВС
*Науковий керівник: старший викладач кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 ХНУВС кандидат юридичних наук Вінцук В. В.*

### СТАНОВЛЕННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

Система охорони державної таємниці (СОДТ) має велике значення для забезпечення національної безпеки будь-якої країни. В Україні у зв'язку із загостренням зовнішньополітичної обстановки, конфліктом на Сході держави проблема ефективності охорони державної таємниці (ОДТ) стає одним із найбільш важливих та актуальних питань на шляху забезпечення національної безпеки. Водночас, вивчення історії становлення та розвитку СОДТ є важливою умовою визначення тих основних рис, які були характерні для певного історичного етапу розвитку СОДТ, з метою їх запозичення або відходження від них з метою вдосконалення СОДТ в Україні.

СОДТ України в історичному аспекті розглядали такі вчені, як О. Абадаш, О. Архипов, О. Ботвінкін, В. Сідак, О. Шамсутдінов та інші.

У своїй науковій праці, Архипов О.Є. приводить наступне тлумачення поняття СОДТ як: створеної у державі для забезпечення ОДТ відповідної системи, основною метою якої є запобігання розголошенню СІ, недопущення втрат її матеріальних носіїв і використання цієї інформації на шкоду безпеці держави. Проаналізувавши вищезазначені та деякі інші точки зору, ми можемо запропонувати таке визначення СОДТ сукупність спеціально уповноважених суб'єктів захисту державної таємниці, використовуваних ними у ході їх діяльності засобів і методів захисту відомостей, що становлять державну таємницю (ДТ), і їх носіїв, а також заходів, що проводяться в цих цілях.

Щодо історичного розвитку СОДТ, то переважна більшість дослідників вважають, що перший етап її розвитку припадає на період кінця XIX – початок XX ст., а завершується в 1917 році з розпадом Російської імперії. Як зазначає О. Абадаш, до середини XIX ст. в Російській імперії (до складу якої входили українські землі), як і в інших країнах світу, не існувало спеціальної системи охорони секретних відомостей, оскільки фактично не було загроз для державної безпеки. Значний економічний розвиток провідних держав світу, їх протистояння за ринки збуту продукції та джерела сировини вплинули і на Російську імперію, зокрема призвели до розробки стратегії і тактики розвідки та контррозвідки.