

Таким чином, для підтримки інформаційно-аналітичної діяльності правоохоронних органів, необхідно знати технологічні засади організації метапошукових систем доступу до документальних інформаційних ресурсів, щоб реалізувати обґрунтовані технології, що охоплюють всі ланцюжки роботи з інформацією, включаючи моніторинг, агрегування та узагальнення потоків інформації.

#### **Список використаних джерел**

1. Додонов А. Г., Ландэ Д. В., Путятин В. Г. Компьютерные сети и аналитические исследования : монография. Киев : ИПРИ НАН Украины, 2014. 486 с.
2. Гришанова І. Ю. Аналітичний огляд методів і засобів інформаційного пошуку в Semantic Web. *Проблеми програмування*. 2016. № 1. С. 51-72.
3. Косиченко О. О. Правові інформаційні ресурси Інтернет : довідник. Дніпро : ДДУВС, 2017. 92 с.

*Одержано 12.11.2020*

УДК 004.056:55(043.2)

**Маляренко Дмитро Сергійович**

*курсант 1 курсу факультету № 4*

*Харківського національного університету внутрішніх справ*

**Гнусов Юрій Валерійович**

*кандидат технічних наук, доцент,*

*завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4*

*Харківського національного університету внутрішніх справ*

<https://orcid.org/0000-0002-9017-9635>

## **ШАХРАЙСЬКІ СХЕМИ, ЯКІ НАЙБІЛЬШ АКТИВНІ В НАШЕ СЬОГОДЕННЯ**

Незважаючи на кризу, стрімко розвивається кредитно-фінансова сфера. Однак вона не завжди приносить користь для громадян, а й часто потурає аферистам, адже інновації в злочинному світі впроваджуються швидко.

*Чорні брокери.* Варто тільки засвітити номер мобільного телефону в інтернеті, наприклад на дошці оголошень, з великою ймовірністю він може потрапити в базу шахраїв, які почнуть регулярно дзвонити, з пропозицією поторгувати, на деякій біржі; або застосовують бота, який буде робити

прогнози та показувати куди ставити. Головним завданням «брокера», буде заставити скачати деяке програмне забезпечення, в який потрібно буде вкладати гроші й торгувати, де й відбудуться осідання. До речі, можуть запропонувати зайти в фішинговий сайт, де результат такий самий – втрата грошей. Позбутися цих дзвінків можна лише змінною SIM-картки.

*Бінарні опціони.* Користуючись соціальними мережами, ми бачимо успішних людей, деякі з них є несправжніми «трейдерами», які готові поділитися торговими сигналами до закритих або відкритих груп, по реферальному посиланню. Зареєструючись і після внесення депозиту, люди починають торгувати по його вказівкам на бінарних опціонах. «Трейдери» заробляють відсотки або за рахунок внесеного депозиту, але, зазвичай, за рахунок поразки жертви. Реклама опціонів може бути де завгодно. Шахраї в онлайн-оголошеннях придумують нові, різні види обману, для привласнення чужих коштів. На дошці оголошень, де розміщуються оголошення про товари, вакансії і резюме, обманюють, як покупців, так і продавців. Шахрай правдоподібно оформлює оголошення з уціненим товаром. Коли на цей товар знаходиться покупець, виникає угода, торгівля. Багато які інтернет - сервіси блокують на своїх сайтах чужі посилання, тому шахрай може попросити перенести спілкування в інші соціальні мережі, мовляв, що там більш зручніше. Вводячи в оману, повідсилає відредаговані, взяті з інших мереж фото чужого товару. Коли покупець повірить, шахрай відсилає посилання на фішинговий сайт, який зовні виконаний по одній стилістиці як справжнє онлайн-оголошення, але відрізняється лише посилання. Обдурений покупець вводить данні своєї банківської карти, номер телефону й відправляє ці данні шахраю, якому буде не складно зняти гроші з карти. Щоб не бути обманутим треба бути уважним, обов'язково читати на сайті інформацію спеціальних розділів, які допомагають впізнати шахраїв.

*SCAM сайти.* Це сайти де, начебто, розігруються грошові кошти: за компенсацію, проходження незначного опитування, тощо. Щоб нібито отримати ці кошти треба оплатити внески, яких буде незчисленна кількість, де і

втратить свої гроші користувач. Скільки б не було проведено транзитних операцій, дані кошти вивести неможливо. Щоб не пійматись на даний проєкт, треба бути скептично налаштованим. На справжніх проєктах з виплати коштів, не треба вносити свої гроші, тому що на всі грошові операції використовуються посередні кошти з виплат.

*НУІР проєкти (фінансові піраміди).* Усі хочуть бути успішними та багатими, найбагатші люди планети рекомендують пасивний заробіток, тобто інвестиція. Існує думка, що кожна людина вчиться на своїх помилках, таким чином, отримуючи безцінний досвід. Але якщо в реальному житті необхідний опит, можна отримати пару раз наступивши на одні і ті, самі граблі, то у інвесторів одна помилка може призвести до втрати всього капіталу. Фінансові піраміди відрізняються від реальних проєктів тим, що у них нема реальної діяльності проєкта. За статистикою, більшість хайпів закривається протягом 6 місяців з моменту свого старту. Не можна при реєстрації використовувати той же e-mail, який ви використовуєте і для платіжних систем. Це може загрожувати тим, що якщо вашу пошту зламують – то паролі від платіжних систем і електронних гаманців зможуть без зусиль відновити і вивести гроші. І саме обов'язкова умова безпеки – для кожного нового проєкту використовуйте різні паролі. Ні в якому разі не застосовуйте один і той же пароль, це може спричинити проблеми. Злом будь-якого вашого облікового запису може дозволити шахраям отримати легкий доступ до акаунтів в інших проєктах, а згодом і крадіжку коштів.

*Вішинг.* Зазвичай телефонні шахраї знаходять номери постраждалих на якомусь форумі або дошці оголошень. Схема надзвичайно проста: шахраї телефонують із незнайомого номера і під різними приводами намагаються: вивідати дані платіжної карти, змусити зняти ліміти на операції по платіжній картці, відключити перевірку коду безпеки картки CVV2 або перерахувати кошти на картку шахраїв. Слід пам'ятати, що ніколи, нікому і ні за яких обставин не можна повідомляти термін дії платіжної картки і трізначний код

безпеки CVV2, а також код підтвердження операції з банківського SMS-повідомлення.

*Висновки.* Багато людей на жаль, думають що в інтернеті заробити гроші без вкладень можна легко і просто, але при пошуку способів заробити грошей, часто потрапляють на шахраїв або шахрайський проєкт, а способів того, як розвести і вкрасти гроші, дуже багато, чорних схем заробітку, сірі і білі схеми є, але чорних більше. Заробити гроші в інтернеті можна, без вкладень, просто треба знати де.

*Одержано 20.11.2020*

УДК 65.012.8 + 004

**Манжай Олександр Володимирович**

*кандидат юридичних наук, доцент,*

*доцент кафедри інформаційних технологій та кібербезпеки факультету № 4*

*Харківського національного університету внутрішніх справ*

<http://orcid.org/0000-0001-5435-5921>

## **ОКРЕМІ АСПЕКТИ УНОРМУВАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ПРАВООХОРОННИМИ ОРГАНАМИ ПІД ЧАС ПРОТИДІЇ ЗЛОЧИННОСТІ**

У Верховній Раді України постійно проводиться робота, щодо унормування використання технологій правоохоронними органами.

На теперішній час в комітеті Верховної Ради України з питань правоохоронної діяльності напрацьовано пропозиції до Кримінального, Кримінального процесуального кодексів України, Кодексу України про адміністративні правопорушення та Законів України «Про оперативно-розшукову діяльність», «Про телекомунікації», у вигляді законопроекту «Про внесення змін до деяких законодавчих актів щодо імплементації положень Конвенції про кіберзлочинність та підвищення ефективності боротьби з кіберзлочинністю». У разі прийняття цього законопроекту, фіксацію електронних доказів можна буде здійснювати за більш логічно обумовленою