URL: https://biz.liga.net/all/it/article/pora-delitsya-v-ukraine-hotyat-vvesti-nalog-na-kriptu (дата звернення: 08.10.2018).

3. В Нацполиции заявили о необходимости запретить криптовалюты в Украине // УНІАН: інформаційне агентство. 29 января 2018 14:51. URL: https://economics.unian.net/finance/2371023-v-natspolitsii-zayavili-o-neobhodimosti-zapretit-kriptovalyutyi-v-ukraine.html (дата звернення: 08.10.2018).

4. Пальчевский И. Украина готовится к легализации криптовалют – НБУ // Financial Club: інформаційне агентство. 16 мая 2018 09:45. URL: https://finclub.net/news/ukraina-gotovitsya-k-legalizatsii-kriptovalyut-nbu.html (дата звернення: 08.10.2018).

Одержано 08.10.2018

УДК 004.056.53

Тетяна Вікторівна ЛИСЕНКО,
магістр факультету № 6
Харківського національного університету внутрішніх справ

КІБЕРЗЛОЧИН ЯК НАЙНЕБЕЗПЕЧНІШИЙ ВИД ЕКОНОМІЧНОГО ШАХРАЙСТВА

Сучасне суспільство інформаційних технологій засновано на повсякденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів комунікації та інших технічних засобів. Щоденне функціонування державних структур, банківської, енергетичної, транспортної та багатьох інших систем неможливо без надійної роботи комп'ютерної техніки та засобів комунікацій. Звичайно, що комп’ютерні системи привернули увагу різного роду шахраїв.

Так, крадіжки даних платіжних карт (банківських рахунків) або даних доступу до системи інтернет-банкінгу з метою заволодіння коштами клієнтів банку, крадіжка персональних даних і комерційної інформації з приватних комп'ютерів або серверів, умисне пошкодження інформаційних систем або засобів комунікацій з метою створення збитків компаніям – це далеко не повний перелік подібних загроз, пов'язаних з бурхливим розвитком сучасних інформаційних технологій.

Результати Всесвітнього огляду економічних злочинів за 2018 рік, підготовленого PwC, свідчать про значне зростання числа респондентів, компанії яких зіткнулися з економічними злочинами, – з 36% в 2016 році до 49% в 2018 році.

Як в Україні, так і в усьому світі найпоширенішим видом економічного злочину є незаконне привласнення активів. В цьому році ми включили в опитування два нових виду економічних злочинів: шахрайство, вчинене клієнтами (32%) і грубе порушення ділової етики (23%). У світі, за даними опитування, рівень даного виду шахрайства знизився з 64% до 45%.

На друге місце вийшли хабарництво і корупція (41% в порівнянні з 30% в 2016 році). Третім найбільш поширеним видом шахрайства є шахрайство в сфері закупівель товарів і послуг. Його відзначили 35% респондентів. Хоча частка респондентів, які відзначили шахрайство в сфері закупівель, практично не змінилася з 2016 року (33%), рівень даного виду економічної злочинності як і раніше стабільний.

На глобальному рівні 31% респондентів відзначили, що їх компанії зіткнулися з кіберзлочинами, які стали другим найпоширенішим видом шахрайства після незаконного присвоєння активів як в 2016, так і в 2018 році. Кількість респондентів в Україні, вказали на кіберзлочини, склало 24%, що менше загальносвітового значення (31%). Причому в порівнянні з 2016 роком ситуація в Україні практично не змінилася: два роки тому цей вид шахрайства відзначили 23% респондентів.

Чи справді респонденти в Україні рідше стикаються з кіберзлочинністю, або технічні можливості кіберзлочинців випереджають можливості їх виявлення?

Високі технології все більше входять в наше повсякденне життя. Ми спостерігаємо зростання поширення цілого ряду «розумних» пристроїв, які можуть контролювати різні процеси в наших будинках, наприклад, освітлення та опалення.

Не дивно, що технології також використовуються для моніторингу економічної злочинності. результати опитувань показують, що в Україні більше компаній задіють технології в якості основного інструменту виявлення економічних злочинів, ніж в світі в цілому, зокрема в таких областях, як виявлення шахрайства (39% і 23% відповідно), протидія хабарництву і корупції (33% і 16% відповідно) і комплексна перевірка благонадійності ділових партнерів (41% і 17% відповідно).

Однак питання ефективності інвестицій компаній в технології як і раніше залишається актуальним. Результати огляду показують, що при оцінці користі, яку приносять компанії інноваційні технології, українські респонденти оцінюють вигоду від таких технологій значно нижче, ніж компанії в усьому світі. Найбільш істотна різниця видна щодо використання такого інструменту як моніторинг електронної пошти. 32% респондентів в Україні використовують цей метод, але не вважають його ефективним, в порівнянні з 10% респондентів на глобальному рівні.

Технології використовуються не тільки для виявлення шахрайства, але і для здійснення економічних злочинів. У Україні 24% респондентів відзначили, що за останні два роки їх компанії постраждали від кіберзлочинів.

Найбільш поширеними злочинами у сфері інформаційних і комп'ютерних технологій є – несанкціоноване списання грошей з банківських рахунків, шахрайство з платіжними картами, втручання в

роботу інтернет-банкінгу, поширення комп'ютерних вірусів, DDoS атаки на інтернет-ресурси, шахрайство в інформаційних мережах.

Таким чином, кіберзлочини вийшли на п'яте місце серед самих поширених видів шахрайства в Україні. Слід зазначити, що за даними глобального огляду цей вид шахрайства посідає друге місце. Приблизно 31% респондентів відзначили, що за останні два роки їх компанії стикалися з кіберзлочинами.

Респонденти всесвітнього огляду згодні з тим, що за своїми наслідками кіберзлочинність стане одним з найбільш руйнівних або серйозних видів шахрайства в найближчі два роки. У Україні 15% респондентів відзначили кіберзлочинність як потенційно саму руйнівну силу, поставивши її на друге місце (в порівнянні з 26% респондентів в усьому світі, які віддали кіберзлочинності перше місце).

Дестабілізація бізнес-процесів є найбільш поширеним типом економічного злочину, вдосконаленим за допомогою кібератаки. Мотиви такого роду атак можуть бути самими різними і вони не обов'язково пов'язані з отриманням ініціатором атаки фінансової вигоди. Це різко відрізняється від ситуації з незаконним привласненням активів, вимаганням і крадіжкою інтелектуальної власності - трьома найпоширенішими цілями кібератак, які набагато частіше спрямовані на отримання фінансової вигоди.

Зростання кіберзлочинності, ймовірно, пояснює значне в порівнянні з 2016 роком збільшення числа респондентів, чиї компанії розробили плани реагування на інциденти. У Україні кількість респондентів, які відзначили наявність в їх компаніях повністю чинного плану реагування на інциденти, зросла з 26% в 2016 році до 62% в 2018 році.

Як показують результати всесвітнього огляду, найчастіше компанії стикаються з таким методом кібератак, як використання шкідливих програм. Використання шкідливих програм вважається одним з найбільш просунутих методів кібератак, що свідчить про зростаючу витонченості кіберзлочинів. Варто також відзначити, що в порівнянні з глобальною статистикою в Україні менш поширені кібератаки, спрямовані на розкрадання персональних даних. Приблизно 33% респондентів всесвітнього огляду відзначили, що їх компанії стали об'єктами атак з метою розкрадання персональних даних за останні два роки, в порівнянні з 20% в Україні.

Остання гучна справа сталася 7 лютого 2018 року, коли Міністерство юстиції США повідомило про пред'явлення звинувачень 36 особам, що входять в кіберзлочинністю групу Infraud, чия діяльність завдала шкоди споживачам, бізнесу і фінансовим організаціям на суму понад $ 530 млн. При цьому хакери мали намір вкрасти більше $ 2,2 млрд.

Серед обвинувачених є громадянин Росії Андрій Новик, а також громадяни України Святослав Бондаренко та Олексій Клименко. При

цьому підкреслюється, що 13 осіб уже заарештовані. Як вказується, це громадяни США, Франції, Італії, Косово, Сербії, Австралії, Великобританії. У Мін'юсті наголошують, що від дій шахраїв постраждали як США, так і інші країни.

У прес-релізі зазначено, що мережа кіберзлочинів, яка функціонує як онлайновий дискусійний форум під назвою Infraud, реалізувала складну схему, яка сприяла купівлі та продажу номерів соціального захисту, днів народження та паролів, викрадених з усього світу. Згідно з обвинувальним висновком, група працювала під гаслом «В шахрайство ми віримо» і була створена в 2010 році Святославом Бондаренко, 34-річним українцем.

В обвинувальному висновку також говориться, що від дій шахраїв постраждали мільйони людей. Так, були вкрадені майже 800 тис. облікових записів доступу в інтернет-банк HSBC, десятки акаунтів PayPal і велика кількість номерів кредитних карт. Крім того, на сайті Infraud можна було розміщувати рекламу шкідливого програмного забезпечення.

Закриття Infraud стане сигналом для інших кіберзлочинців, однак навряд чи серйозно знизить їх активність, оскільки в інтернеті існують близько 200 аналогічних форумів, багато з яких мають набагато більшу аудиторію, говорять в компанії Recorded Future, що спеціалізується на кібербезпеці.

Висновок. За прогнозами, кіберзлочинність стане одним з найбільш руйнівних видів шахрайства в найближчому майбутньому. хоча у більшості компаній є план дій в разі порушення кібербезпеки, але лише деякі з них провели оцінку кіберризиків.

Одержано 06.11.2018

УДК 004.6

Костянтин Євгенійович ЛИТВИНОВ,
провідний фахівець сектору безпеки
філії УкрНДІгаз АТ «Укргазвидобування»

АНАЛІЗ ТА СИСТЕМАТИЗАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ

Одна з найважливіших проблем у протидії з кіберзлочинністю та торгівлею людьми тісно пов’язана з накопиченням та аналізом персональних даних громадян. В сучасному світі ми майже не зустрічаємо людину, яка б не мала жодного аккаунту в соціальних мережах, мобільних додатках, інтернет-магазинах або онлайн банках.

Поняття накопичення персональних даних необхідно розглядати у двох аспектах: як пошук інформації з відкритих джерел інформації (використання методології пошуку OSINT) та систематизація персональних даних в єдине джерело з офіційних джерел інформації.