носій, має лише номер за відсутності серії. Тому під час заповнення суб'єктом первинного фінансового моніторингу форми 2ФМ відповідний реквізит набуває значення константи ZZZZZ.

Література:

1. Держфінмоніторинг виявив фінансові операції на 45,2 млрд гривень, які можуть бути злочинними [Електронний ресурс]: – Режим доступа:http://www.kmu.gov.ua/control/uk/publish/article?art_id=250351332&cat_id=244277212

2. Науково-практичний коментар до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» / Чубенко А.Г., Лошицький М.В., Бичкова С.С., Котляревський Я.В.– К.: Ваіте, 2015. – 816 с.

Актуальні питання боротьби з кіберзлочинністю в Україні

Новіцький О.І.
студент 4 курсу факультету №4
Олексієнко А.
Студентка 3 курсу ПОД Факультету №4.
Науковий керівник: Косаревська О.В.
кандидат педагогічних. наук, доцент, доцент кафедри кібербезпеки та інформаційного забезпечення ОДУВС

В світлі стрімкого розвитку суспільства та глобальній інформатизації всіх сфер діяльності актуальною проблемою постає боротьба з кіберзлочинністю, як на національному рівні так і на міжнародному. Злочинні організації (так само як і окремо взяті злочинці) все частіше стали звертатися до мережі Internet з метою полегшення своєї діяльності і збільшити свій прибуток в найкоротші терміни. Хоча самі по собі злочини не обов'язково нові, але вони розвиваються з новою силою, оскільки ступінь контролю правоохоронних органів мережі Internet менший, а можливостей, наданих мережею Internet, надзвичайно багато, тому саме кіберзлочини стають все більш масовими і руйнівними.

Сучасний стан кіберзлочинності в Україні містить кримінологічний аналіз показників кіберзлочинності. Аналіз даних офіційної статистичної звітності за останні чотирнадцять років свідчить про тенденцію стабільного та стрімкого зростання рівня кіберзлочинів. Їх середньорічний рівень:

- 2002–2015 рр. склав 205 злочинів.
- у 2015 році абсолютна кількість зареєстрованих кіберзлочинів сягнула 556, що на 1753,3 % більш ніж у 2002 році та на 33 % більше ніж у 2014.
- середньорічний темп приросту протягом 2002–2015 рр. склав 107,5 %.

Опираючись на данні про кількість зареєстрованих в розрізі регіонів України упродовж 2016 року злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361-363-1 КК України) та результати їх досудового розслідування та аналогічні данні за перший квартал 2017 року, наданні Генеральною Прокуратурою України очевидно, що проблема кіберзлочинності надзвичайно актуальна, оскільки за 2016 рік кіберзлочинів було вчинено 1018, а за перший звітний квартал 2017 року – 705. Ми бачимо великі темпи росту кіберзлочинності, що тягне за собою низку проблем, які потрібно першочергово вирішувати зважаючи на темпи росту даного виду злочинності.

Спираючись на дослідження кримінологів, психологів, юристів в сфері протидії кіберзлочинності, що відбилося у роботах провідних фахівців: Бутузова, Тихомирова, Кудінова В.А., Г. Ю. Маклакова.

Деякі аспекти нормативної бази по боротьбі з кіберзлочинності вивчали та обговорювали в своїх публікаціях К. Бєляков, В. Бутузов, А. Волеводз,Д. Гавловський, В. Голубєв, В. Гуславський Д. С. Кльоцкін, М. Литвинов, Е. Рижков, В. Розовський Т. Тропина, В. Цимбалюк, О. Юхно та інші.

У науковій літературі боротьба зі злочинністю розглядається як першочергове загальнодержавне завдання, яке є складовою частиною діяльності органів державної влади і, насамперед, Національної поліції. Особливе місце в боротьбі зі злочинами, пов'язаними з протиправним використанням комп'ютерної інформації та комп'ютерних технологій, необхідно надати правоохоронним органам України [3, с. 219].

На сьогодні в Україні діє низка законів та нормативних документів різних рівнів, що охоплюють питання кібербезпеки держави. Це, зокрема, Закони України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», Указ Президента України «Про Національний координаційний центр кібербезпеки» та інші нормативно-правові акти. Крім того, у вересні 2016 року Верховна Рада України прийняла у першому читанні Закон України «Про основні засади забезпечення кібербезпеки України».

Стратегічними документами у цій сфері є: Стратегія кібербезпеки України, Стратегія національної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність». Чинний Кримінальний кодекс України встановлює (відповідно до розділу XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Всі міжнародні організації відзначають необхідність скоординованої міждержавної взаємодії при розслідуванні кіберзлочинів. Саме завдяки роботі таких міжнародних організацій, як Організація економічного співробітництва і розвитку, Інтерпол, Група Восьми, Рада Європи, ООН розвивається міжнародна співпраця країн у сфері боротьби з кіберзлочинністю, формується міжнародне законодавство.

Відповідно до ст. 23 Конвенції про кіберзлочинність , сторони співпрацюють між собою у найширших обсягах шляхом застосування відповідних міжнародних документів щодо міжнародного співробітництва у кримінальних питаннях, угод, укладених на основі єдиного чи взаємного законодавства, і внутрішньодержавного законодавства з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень.

Для подолання кіберзлочинності на національному рівні в структурі Державної служби по боротьбі з економічною злочинністю при МВС України в 2001 році були створені підрозділи по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій, одним із завдань котрих є боротьба із злочинами у галузі комп'ютерної інформації, електронних рахунків телекомунікації.

Наступною сходинкою для подолання кіберзлочинності було створення 5 листопада 2015 року нової Кіберполіції, як структурного підрозділу Національної поліції. Основною метою створення кіберполіції було реформування та розвиток підрозділів МВС України, що забезпечить підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності [1].

Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України та згідно із законодавством України здійснює оперативно-розшукову діяльність.

Департамент діє на основі поєднання єдиноначальності та колегіальності у вирішенні питань оперативно-службової діяльності, перспективного й поточного планування, а також своєчасного і якісного виконання планових заходів, наказів, рішень і доручень керівництва Національної поліції України та МВС, з урахуванням наукових рекомендацій та передового досвіду, у тому числі міжнародного.

До основних завдань кіберполіції відносять:

- реалізація державної політики у сфері протидії кіберзлочинності;
- протидія кіберзлочинам;
- завчасне інформування населення про появу новітніх кіберзлочинів;
- впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кібер злочини;
- реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів;
- участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності;
- участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

Проблема профілактики кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою.

Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній [2].

Першою причиною розвитку кіберзлочинності є прибутковість, – вона неймовірно прибуткова. Величезні суми грошей з'являються на рахунках злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть простим потоком.

Друга причина росту кіберзлочинності як бізнесу - те, що успіх справи не пов'язаний з більшим ризиком. У реальному світі психологічний аспект злочину припускає наявність деяких коштів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, чи то окремі люди, чи то цілі організації, які вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше [2]. У кожного покоління злочинців свої інструменти. Сучасні кіберзлочинці вибрали своєю зброєю троянські програми, за допомогою яких вони будують бот-мережі для крадіжки паролів і конфіденційної інформації, проводять Dos атаки й шифрують дані, щоб потім шантажувати.

Характерною й небезпечною рисою сьогоднішніх шкідливих програм є те, що вони прагнуть зберегти свою присутність на «інфікованій машині». Для досягнення цієї мети злочинці використовують різні технології. Інша розповсюджена технологія, використовувана в шкідливих програмах, - порушення роботи антивірусних програм для запобігання виявлення шкідливого ПО й продовження його існування на комп'ютері. Такі дії часто спрямовані на припинення забезпечення безпеки, видалення коду або модифікацію хостових файлів Windows для припинення відновлення антивірусних. Серед установ, які намагаються максимально швидко брати на озброєння технологічні новинки, чільне місце посідають банки. Вони мало не щомісяця пропонують нам сервіси, що дозволяють максимально легко і просто розпоряджатися своїми грошима. Платіжні карти і банкомати вже давно стали частиною нашого життя, а інтернет-банкінг, купівля товарів через всесвітню мережу – це те, що ми використовуємо по всяк час. На жаль, цим користуються не лише клієнти, а й злочинці.

В сфері боротьби з кіберзлочинами кожний з нас також може зробити свій вклад за рахунок дотримання простих правил, які значно можуть обтяжити діяльність кіберзлочинців. Спираючись на дані інтернету, ми можемо знайти масу правил, стосовно кібербезпеки.

До таких правил можна віднести наступне [4].

- Створюйте надійні паролі та періодично їх змінюйте.

Щоб створити такий пароль і при цьому його не забути, доцільно запам'ятати кілька слів та цифр, де кількість символів має бути не меншою від 8. При цьому у фразі можна замінити окремі літери, умисно створивши помилки, і ввести з клавіатури, попередньо перемкнувши її розкладку на іншу мову.

- Користуйтесь антивірусним програмним забезпеченням. Обов'язкова умова - його постійне оновлення.
- Працюйте з комп'ютером у режимі користувача. Цією порадою нехтують найчастіше. Якщо після встановлення операційної системи ви продовжуєте для зручності використовувати комп'ютер в режимі «Адміністратор», цим ви створюєте додаткові ризики зараження комп'ютера вірусами, які пропустила антивірусна система.
- Виявляйте обережність при спробі підвищити власну анонімність. Окремі користувачі, намагаючись залишити якнайменше слідів свого перебування в мережі Інтернет, застосовують анонімайзери, безкоштовні проксі-сервери або програмні додатки типу TOR. Більшість цих ресурсів є вільними та безоплатними. Утім, користуючись ними, ви залишаєте повний комплект інформації (логін/пароль), достатньої для несанкціонованого доступу до вашої сторінки. Таким чином, питання щодо того, скористатися чи не скористатися цією можливістю, ви залишаєте на розсуд власників цих анонімайзерів. Така ж сама ситуація з використанням вільних точок доступу WI-FI.
- Завжди контролюйте інформацію, яку ви розміщуєте на власній сторінці у соціальній мережі. Надлишкова відкритість щонайперше може бути використана при підготовці протиправних дій стосовно вас.
- Візьміть за правило не відкривати посилання, що надходять вам у повідомленнях на сторінці. Краще копіюйте їх і вставляйте у пошукову сторінку браузера в якості тексту.

Підсумовуючи вищевикладене, можемо дійти таких висновків:

- поширеність і суспільна небезпечність кіберзлочинів останніми роками набула загрозливих масштабів, що диктує необхідність формування адекватної відповіді з боку держави;

- вивчення зарубіжного досвіду протидії кіберзлочинності в окремо взятих країнах і надбань міжнародної спільноти, удосконалення механізму міжнародної взаємодії є важливим, адже більшість кіберзлочинів мають транснаціональний характер;
- кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а загрожує людству загалом, саме тому зазначеній проблемі приділяється значна увага в багатьох державах;
- з огляду на сучасну ситуацію в державі та світі, Україна має постійно вдосконалювати методи боротьби з кіберзлочинністю, удосконалюючи чинне законодавство, у тому числі в галузі адміністративного права, враховуючи надбання окремих зарубіжних держав, міжнародної спільноти загалом, спрямовані на забезпечення кібербезпеки країни;
- важливим є прийняття Закону, який би врегулював основні засади забезпечення кібербезпеки України.

Література

1. Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» http://zakon2.rada.gov.ua/laws/show/96/2016.
2. Солодка О. М. Боротьба з комп'ютерною злочинністю як пріоритетний напрям забезпечення інформаційної безпеки України / О. М. Солодка //Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., 17 берез. 2010 р., м. Київ. – К.: Нац. акад. СБУ України, 2010. – С. 126-128
3. Перепелиця М. М. Кіберпростір і оперативно-розшукова діяльність / М. М. Перепелиця, О. В. Манджай // Вісн. Луган. держ. ун-ту внутр. справ. Луганськ, 2008. – Ч.1, Спец. вип. 1.
4. Кіберзлочинність у всіх його проявах:види, наслідки та способи боротьби [Електронний ресурс] http://gurt.org.ua/articles/34602/.

Електронний цифровий підпис: персоніфікація та захист

Олашина А.О.
викладач правознавчих дисциплін
ДВНЗ ОКЕПГРБ

Можливість захистити свої електронні данні в епоху достатньо стрімкого розвитку інформаційних технологій є не тільки абстрактною можливістю, «умовною опцією», яка використовується, а й вже сучасним необхідним правовим аспект гарантії належного збереження електронних документів з урахуванням їх законної юридичної сили.

Ст. 8 Закону України "Про електронні документи та електронний документообіг" передбачає, що юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму, але задля того, щоб електронний документ відповідав вимогам, які висуваються чинним законодавством та мав статус такого, що має законну юридичну силу, він повинен бути підписаний електронним цифровим підписом [1].

Задля того, щоб визначитись в чому полягає суттєва відмінність між електронним цифровим підписом та електронним підписом, звернемось до Закону України «Про електронний цифровий підпис», який і надає визначення. Так, електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних [2]. Тобто, електронний підпис, на відміну від електронного цифрового підпису є таким, що не захищає особисті данні особи, він може виявлятись у згоді особи з правилами та умовами певного сайту, у погодженні відповідної особи з передачею її особистих даних третій особі, наприклад, при вчиненні online-замовлення, тобто електронний підпис не створює підстав задля створення умов персоніфікованого захисту даних відповідної особи.

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [2]. На відміну від електронного підпису, електронний цифровий підпис (далі – ЕЦП) дає можливість не тільки ідентифікувати особу, що використала цей підпис, але й захистити зміст даних, які знаходяться у документі, захищеному ЕЦП. Використання ЕЦП вже створює умови для