органів [3].

Отже, можемо констатувати, що спільними зусиллями влади і компетентних органів можна суттєво обмежити тіньову складову сфери зовнішньоекономічної діяльності, мінімізувати втрати бюджету від контрабанди товарів до України та спрямувати додаткові фінансові надходження до централізованих та децентралізованих фондів коштів. Аналіз показує, що навіть фрагментарні та непослідовні спроби наведення ладу в цій сфері практично одразу дають відчутний позитивний ефект у формі збільшення надходжень до Держбюджету.

Використані джерела

1. Перепелица А. И. Уголовно-правовая борьба с организованной преступностью в сфере хозяйственной деятельности / А. И. Перепелица // Правові проблеми боротьби зі злочинністю. – 2002. Книга 2. – С. 154.
2. Зелинский А. Ф. Понятие «преступная деятельность» / А. Ф. Зелинский // Сов. государство и право. – 1978. – № 10. – С. 98–100.
3. Щодо єдиного порядку обліку злочинів у сфері економіки: (Спільна вказівка Ген. прокуратури, МВС, ДПА та Служби безпеки України від 02.06.2004 р. № 12-157) [Електронний ресурс]. – Режим доступу : stat@uvddon.donec.ua
4. Документування злочинних дій хабарників: [методич. рекомендації] / за ред. В. І. Литвиненка ; [упоряд.: В. С. Гарлицький, О. О. Дульський, В. М. Конорєв, В. Б. Моцар]. – К. : РВВ МВС України, 2001. – 80 с. – С. 6.
5. Загрози без кордонів [Електронний ресурс] / Український Інтерпол: шляхом розвитку. – Режим доступу : http://www.niss.gov.ua/Tasko/017.htm
6. Про рішення РНБОУ від 11 верес. 2009 р. «Про стан злочинності у державі та координацію діяльності органів державної влади у протидії злочинним проявам і корупції» : Указ Президента України від 27 жовт. 2009 р. № 870/2009 [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua
7. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. – [6-те вид., переробл. та доповн.]. – К. : Юридична думка, 2009. – 1236 с.

Хоменко В.М. , Савченко В.О. - студентки юридичного факультету; науковий керівник: **Косиченко О.О.** – доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ПРОБЛЕМИ ЛАТЕНТНОСТІ КІБЕРЗЛОЧИННОСТІ

У зв’язку із розвитком всесвітньої мережі Інтернет з’явився новий вид злочинності, а саме – кіберзлочинність. З кожним днем вона набирає оберти та несе за собою незворотні наслідки. Дана проблематика загострює необхідність боротьби зі злочинами такого роду: створення комп’ютерних систем, технологій з підвищеним рівнем безпеки в мережі, законодавчої бази,

незаконного обігу інформації, поширення не ліцензованого програмного забезпечення для комп'ютерів.

Теоретико-методичні та науково-практичні основи попередження дій кіберзлочинців були закладені у дослідженнях таких науковців: В. Голубєва, А. Долгової, К. Касперськи, М. Кастельса, Т. Кесаревої, Л. Куракова, Р.Лемоса, А. Лукацького, І. Рассолова, С. Смірнова.

Термін «кіберзлочинність» у нормативних документах невизначений. Концепція даного визначення була сформована завдяки діяльності правоохоронних органів розвинутих країн Європи та світу.

Латентна злочинність – це частина злочинності, яка складається зі злочинів, що фактично були вчинені, але не отримали відображення у офіційній загальнонаціональній кримінально-правовій статистиці.

Якщо розглядати види латентності злочинності, то до них слід віднести наступні:

1. *Природна (прихована) латентність* – це сукупність злочинів, про вчинення яких не стало відомо компетентним органам та інформація про які не відображена відповідним чином у офіційній кримінальній статистиці. Причинами цього виду латентності може бути, зокрема, відсутність потерпілого та свідків злочину (т. 3. "злочини без жертви"), незначна шкода, заподіяна злочином, небажання потерпілого заявляти про вчинений щодо нього злочин (наприклад, внаслідок родинних відносин із правопорушником або через почуття сорому чи страху), вдале приховання злочинцем слідів злочину тощо.
2. *Штучна (приховувана) латентність* – це сукупність злочинів, відомості щодо яких надійшли до правоохоронних органів, але при цьому реєстрації останніми події злочину не відбулося. Причинами виникнення штучної латентності можуть бути відмова у реєстрації заяви про злочин, помилкова або умисно невірна кваліфікація вчиненого як некримінального (цивільно-правового, адміністративного, дисциплінарного) правопорушення.
3. *Суміжна (межова, прикордонна) латентність* – це сукупність злочинів, які не оцінюються потерпілими як вчинені щодо них протиправні діяння. Причинами цієї латентності може бути необізнаність громадян із положеннями кримінального закону, вплив на оцінку вчиненого специфічних традицій певної місцевості тощо.

До подій, пов'язаних зі злочином можна віднести ситуації, при яких комп'ютер – знаряддя для вчинення злочинів, з метою порушення авторських прав, громадської безпеки, прав власності, моральності.

<u>*Класифікація кіберзлочинів:*</u>

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема: - незаконний доступ, наприклад, шляхом злому, обману та іншими засобами; - нелегальне перехоплення комп'ютерних даних; - втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; - втручання у систему, включаючи умисне створення серйозних

перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру; - зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних програм, комп'ютерних паролів або кодів доступу метою здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

У той же час, з урахуванням мотивації злочинців, кіберзлочини представляється можливим умовно розділити на наступні категорії: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення шкоди конкурентам); інші злочини.

Ознайомившись з інформацією наданою вище можна зрозуміти, що кіберзлочини відрізняються від інших тим, що вони здійснюються за допомогою сучасної техніки (інтернет, комп’ютери, операційні системи, модернізована електронна техніка, тощо).

У 2008 році в десятці найбільш небезпечних загроз, що відзначаються фахівцями, були мережі ботів - «цілеспрямовані» атаки на урядові сайти, приватні підприємства та кінцевих користувачів. А в 2013 році, згідно прогнозом фахівців McAfee, на перший план вийшли загрози, пов`язані звикористанням мобільного доступу в Мережу.

Злочинність в кіберпросторі - одна з найгостріших проблем, з якою зіткнулося міжнародне співтовариство протягом останніх десятиліть у зв`язку з розвитком інформаційних технологій.

Щоб уявити собі масштаби і обороти цього кримінального бізнесу, досить навести деякі приклади. Віртуальні шахраї, заволодівши через Мережу номерами більш ніж мільйона банківських карт - громадян США, одночасно зробили розкрадання в 130 банкоматах в 49 містах Америки. При цьому вся операція зайняла не більше 30 хвилин, а розмір прибутку злочинців склав близько 9 млн. доларів, які потім були переведені на рахунки в різні держави, в основному в пострадянському просторі. У 2010 р. ФБР висунуло звинувачення проти 37 жителів Росії, України та інших східноєвропейських країн, підозрюваних у використання комп`ютерного вірусу для злому американських банківських рахунків.

Найбільш поширені злочини, які відносяться до другої і третьої категорії – це злом баз даних і виведення з ладу комп'ютерних систем

компаній і державних організацій, а також крадіжка інновацій або технологій.

На нашу думку, кіберзлочинність можливо охарактеризувати наступним чином – це злочинність, так званому «віртуальному просторі», яка змодельована за допомогою сучасної техніки. На сьогодні на електронних носіях та електронних базах знаходиться відомості про осіб, предмети, факти, події, явища та процеси.

Законодавство України, в особах голови держави та інших посадових осіб згідно діючого законодавства прагне захистити своїх громадян та мінімізувати кількість постраждалих від даного злочину.

Тому у 2016 р. Указом президента була затверджена Стратегія кібербезпеки України, а пізніше відбулося підписання Указу про створення Національного координаційного центру кібербезпеки. У вересні 2016 року Верховна Рада України у прийняла Закон "Про основні засади забезпечення кібербезпеки України".

Дуже важливим фактом є те, що національний законодавець закріпив у Кримінальному Кодексі України у розділі XVI злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. В Кримінально-процесуальному Кодексі також закріплені положення щодо злочинів в сфері ІТ-технологій. Та все ж таки тих норм, що закріплені в чинному законодавстві недостатньо, і вони не завжди є ефективними.

Останнім часом в Україні постало нове, дуже серйозне випробування; яке поширюється досить стрімко. Це створення таких інтернет-банд як "Синій кит", "Тихий дім", "Кити пливуть Вгору", "Море китів", "Біжи або помри", "Розбуди мене в 4.20", F57, F58, FF33, D28 тощо. Метою таких сайтів є пропаганда самогубства серед дітей та підлітків. Слід зазначити, що жертвами стають діти, в яких є проблеми з батьками, з друзями в школі, тобто особливо вразливі діти, які не отримують необхідної уваги та любові.

Однією з головних проблем, чому злочини в сфері інформаційних технологій мають низький рівень розкриття, є те, що людям не вистачає спеціальних знань. У зв'язку з тим, що бурхливий розвиток інформаційних технологій методики судово-експертного дослідження даних об'єктів вимагають постійного оновлення та доопрацювання. Кожного року змінюються операційні системи, формати даних, протоколи і середовище перенесення даних, технічні засоби, що забезпечують процеси передання та обрабки інформації.

Сліди кіберзлочинів досліджуються за допомогою комп'ютерно-технічної експертизи та експертизи відео- та звукозапису. А щодо наукової експертизи, то він повністю залежить від рівня професійної підготовки експертних кадрів. У світі досить ретельно підходять до проблеми боротьби з кіберзлочиннами, і до її вирішення безпосередньо залучається державна влада. Адже ту кількість інформації, яка протікає по мережі Інтернет щоденно, просто нереально контролювати самостійно. Тому, починаючи з 2009 року, влада США розпочала створення власних кібервійськ — Агенство

національної безпеки, яке також опікується питаннями інформаційної війни. У ЕС функціонує Агенство з мережевої та інформаційної безпеки, у НАТО створений комітет з кібернетичної оборони, а також Спільний центр з кібернетичної оборони.

Так, відомий російський виробник антивірусного програмного забезпечення "Лаборатория Касперского" за останні роки виявив декілька бойових вірусів, які є настільки складними, що їх розробкою, без сумніву, фундаментально і багато часу займалися великі за чисельністю групи фахівців найвищої кваліфікації, а вартість розробки цих шкідливих програм оцінена в 100 мільйонів доларів США. Один з таких вірусів уже був застосований в Іраку під час бойових дій.

Під час інформаційних війн зброєю виступають засоби масової інформації, соціальні мережі, "тролінг" та блогсфери. Що стосується України, то в даній країні відсутні власні майданчики для обміну інформації (Facebook, Twitter, YouTube, Вконтакте, Однокласники тощо) на відміну від зарубіжних країн, також країна не підтримує національні елетронні програми, ми не випускаємо власних електронних приладів тощо. А це означає, що ми дуже вразливі під час будь-якої інформаційної війни. Кіберзлочинність в Україні розвинена чи не найвище серед усіх європейських країн. Ми вважаємо, що наша держава повинна приділити набагато більше уваги даному питанню, дана прогалина робить нас дуже вразливими.

Для забезпечення кібербезпеки існують різноманітні міжнародні договори, так у 2002 році Організація Об'єднаних Націй видала резолюцію Генеральної Асамблеї, де були прийняті "Елементи для створення глобальної культури кібербезпеки". В документі зазначається 9 основних взаємодоповнюючих елементів, які держави-учасники повинні дотримуватися, серед них: обізнаність, відповідальність, реагування, етика, демократія, оцінка ризику, проектування та впровадження засобів забезпечення безпеки, управління забезпеченням безпеки та переоцінка.

Підсумовуючи усе вище зазначене, вважаємо за доцільне підкреслити наступні моменти: ми маємо неймовірний світ сучасних технологій, які повинні працювати на благо людей. Все, що іде всупереч засадам демократичного суспільства, повинно бути засуджено за законом, тільки через відповідну законодавчу базу справедливий неупереджений суд в суспільстві встановлюється справедливість і порядок. необхідно внести деякі доповнення до Кримінального Кодексу України, які будуть гарантувати кібербезпеку людей. До таких злочинів можна віднести : дефейс, шантажування, вбивство, екстремізм в мережі, наклеп, образи, фішинг, комп'ютерне шпигунство тощо.

Використані джерела

1. Бондаренко О. С. та Рєпін Д. А. – Кіберзлочинність в Україні: причини, ознаки та заходи протидії - [Електрон. ресурс] / Режим доступу: http://www.pap.in.ua/1_2018/73.pdf

2. В. Б. Дзюндзюк та Б. В. Дзюндзюк – поява та розвиток кіберзлочинності – [Електрон. ресурс] / Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf
3. Панфілов О. Ю. – До проблеми оцінки сучасного рівня інформаційної безпеки України – Зовнішня торгівля: право, економіка,фінанси, № 3 – 2012 [Електрон. ресурс] / Режим доступу: http://zt.knteu.kiev.ua/files/2012/03(62)2012/3_12_34.pdf

Цісар Б.О. - курсант факультету економіко-правової безпеки; науковий керівник – **Кокарєв І.В.** - доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук, доцент (Дніпропетровський державний університет внутрішніх справ)

ЕКОНОМІЧНА БЕЗПЕКА В УКРАЇНІ

Проблемність економічної безпеки в умовах подальшої глобалізації набуває статусу найвищого пріоритету в державній політиці. Виняткове значення вона має при аргументації прийняття політичних рішень. Науково-концептуальні засади про економічну безпеку забезпечують формування відповідної політики на рівні держави чи суб'єктів нижчих організаційних рівнів. Система забезпечення економічної безпеки передбачає здійснення постійного моніторингу соціально-економічних процесів з точки зору їхнього впливу на стан економічної безпеки, оцінку з цих позицій стратегічних програм, нормативно-правових актів, а також аналіз ефективності поточних рішень у сфері економічної політики.

Термін «національна безпека» започатковано США, який вперше офіційно було використано Президентом Сполучених Штатів Теодором Рузвельтом. У своєму посланні Конгресу в 1934 р. він виправдовував захоплення зони майбутнього Панамського каналу інтересами «національної безпеки США». У 1947 р. Конгресом США було прийнято закон «Про національну безпеку». Відтак проблема національної безпеки стала однією із стрижневих у наукових дослідженнях американських і західноєвропейських учених у соціологічній, політологічній та економічній галузях. Після Другої світової війни США вирішили максимально використати тогочасні можливості свого впливу. Саме тоді американці й розробили концепцію національної безпеки, а на її основі — доктрину державної безпеки. Закон США «Про національну безпеку» зобов'язав усі державні структури провадити цілеспрямовану політику щодо воєнно-політичного протистояння з Радянським Союзом та державами Варшавського договору [1].

У науковій літературі наводиться багато поглядів на визначення поняття «економічна безпека держави». Визначення вітчизняних та зарубіжних фахівців відрізняються різноманітністю підходів і суттєво розбігаються за змістом [2]. Зокрема, на думку Л.І. Дмитриченка, економічна безпека — це стан держави, за якого вона має можливість створювати і розвивати