6. Гора І.В. Криміналістика: посіб. [для підготов, до іспитів] / І.В. Гора, А.В. Іщенко, В.А. Колесник. – 2-е вид., допов. та переробл. – К.: Вид. Паливода А.В., 2004. – 223 с.

7. Гутерман М.П. Организационные мероприятия следователя в процессе расследования преступлений (уголовно-процессуальное и криминалистическое исследование): автореф. дис. на здобуття наук. ступ. канд. юрид. наук: спец. 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» / М.П. Гутерман. – М.: Академия МВД СССР, 1980. –26 с.

8. Клюс В.В. Проблеми протидії умисним вбивствам вчинених на релігійному ґрунті / В.В. Клюс // Правова система: сучасні проблеми та перспективи розвитку: матеріали конференції. VII Всеукраїнської науково-практичної конференції (22 жовтня 2010 р.) / відп. ред. О.М. Барно. – Кіровоград: Видавництво КІРоЛ "Україна", 2010. – С. 17-23.

9. Бахин В.П. Допрос: лекція / В.П. Бахин. – К.: КГУ, 1999. – 40 с.

10. Подголин Е.Е. Тактика следственных действий: учебно-практическое пособие. – К.: Правник, 1997. – 71 с.

УДК 351.749: 343.451 (100)

ПИТАННЯ ДІЯЛЬНОСТІ СПЕЦІАЛЬНИХ ПІДРОЗДІЛІВ ПО БОРОТЬБІ З ІНТЕРНЕТ-ШАХРАЙСТВОМ У ЗАРУБІЖНИХ КРАЇНАХ

Сабадаш В.П., к.ю.н., доцент

Запорізький національний університет

У статті розглядаються актуальні питання створення та функціонування спеціальних підрозділів по боротьби із інтернет-шахрайством у зарубіжних країнах задля запозичення накопиченого досвіду в діяльності правоохоронних органів України.

Ключові слова: інтернет-шахрайство, боротьба, спеціальні підрозділи, розслідування, злочин, кіберзлочинність, інформаційні технології.

Сабадаш В.П. ВОПРОСЫ ДЕЯТЕЛЬНОСТИ СПЕЦИАЛЬНЫХ ПОДРАЗДЕЛЕНИЙ ПО БОРЬБЕ С ИНТЕРНЕТ-МОШЕННИЧЕСТВОМ В ЗАРУБЕЖНЫХ СТРАНАХ / Запорожский национальный университет, Украина

В статье рассматриваются актуальные вопросы создания и функционирования специальных подразделений по борьбе с интернет-мошенничеством в зарубежных странах для дальнейшего заимствования накопленного опыта в деятельности правоохранительных органов Украины.

Ключевые слова: интернет-мошенничество, борьба, специальные подразделения, расследование, преступление, киберпреступность, информационные технологии

Sabadash V.P. ISSUES OF SPECIAL UNITS TO COMBAT INTERNET FRAUD IN FOREIGN COUNTRIES / Zaporizhzhiy national university, Ukraine

The article deals with current issues of creation and functioning of special units to combat Internet fraud in foreign countries for further borrowing of experience in the law enforcement bodies of Ukraine.

It is stated that in the world today is the creation of special organizations involved in various aspects of the fight against Internet fraud, which can be roughly divided into three groups:

1) state special organization, responsibilities which include the issues of combating crime in the sphere of high technologies;

2) non-state interagency organizations that are engaged in registration of complaints of criminal activities online orientation;

3) special organizations and departments that are created within the framework of international or interstate institutions.

So, the first group of special organizations include the organization and management created by the state as part of the central government: Ministries, agencies, security services etc.

The second group of special organizations and expert groups involved in the study of computer incidents, and registering complaints against the criminal actions of Internet-oriented, acting as intermediaries between users

of the Internet and special state organizations involved in combating computer crime in general, and Internet fraud in particular.

There are three main types of expert groups that exist in the world and were investigating incidents of computer and Internet security, namely:

1) Computer Emergency Response Team, CERT;

2) Computer Security Incident Response Team, CSIRT);

3) Computer Emergency Readiness Team.

In addition, in the world are being already established international associations CSIRT / CERT centers, such as the Forum of Incident Response and Security Teams (FIRST) and the Trusted Introducer – community, bringing together European teams to respond to information security incidents.

No doubt, the experience of leading countries in the collection, research and exchange of information about computer incidents and cyber threats may well be used in Ukraine by creating online databases of incidents and the Center for Internet crime complaints similar to the IC3 (Internet Crime Complaint Center – USA) and RU CERT (Center for Response at Computer Incidents In Russian Federation).

Key words: Internet fraud, fight, special units, investigation, crime, cybercrime, information technology.

Сьогодні у повсякденному житті використовується безліч різноманітних високотехнологічних пристроїв – пластикових карток, мобільних телефонів, планшетів, комп'ютерів. Постійно з'являються нові моделі, програми та сервіси. Все це робить наше життя кращим, але потребує певних навичок та знань. Суспільство стало більш технологічно залежним.

Разом із розвитком високих технологій, з'являються нові види шахрайств, направлені на присвоєння грошових коштів громадян, що ставить перед суспільством та правоохоронними органами завдання протидії таким шахрайським проявам. Особливо це стосується глобальної мережі Інтернет, яка не знає кордонів, тому дозволяє шахраям на відстані здійснювати свої злочинні наміри. З'явився навіть такий термін як «Інтернет-шахрайство».

Отже, метою цієї статті є необхідність дослідження питань створення та функціонування спеціальних підрозділів по боротьби із інтернет-шахрайством у зарубіжних країнах задля запозичення накопиченого досвіду в діяльності правоохоронних органів України.

Вивчення стану наукової розробленості проблеми протидії інтернет-шахрайству шляхом створення спеціальних підрозділів по боротьби з таким проявом злочинних посягань показало, що на сучасному етапі спеціального дослідження із цих проблем не проводилося. Проте необхідно зазначити, що окремі аспекти протидії комп'ютерній злочинності розглядалися в роботах Д.С. Азарова, Ю.М. Батурина, П.Д. Біленчука, М.С. Вертузаєва, В.Б. Вєхова, В.О. Голубєва, М.Д. Дихтяренко, Є.І. Панфілової, О.М. Попова, Н.А. Селіванова й деяких ін.

Необхідно зазначити, що на сьогоднішній день у світі вже створені спеціальні організації, які займаються різними аспектами боротьби із Інтернет-шахрайством.

Всі ці спеціальні органи умовно можна поділити на три великі групи:

1) державні спеціальні організації, у функціональні обов'язки яких входять питання боротьби зі злочинами у сфері високих технологій;

2) недержавні міжвідомчі організації, які займаються реєстрацією скарг на злочинні дії Інтернет спрямування;

3) спеціальні організації та департаменти, що створюються в рамках діяльності міжнародних чи міждержавних інституцій.

До першої групи спеціальних організацій відносяться організації та управління, які створюються державами у складі центральних органів влади: Міністерств, відомств, Служб безпеки тощо.

Так, в Російській Федерації – це Бюро спеціальних технічних заходів МВС Росії, до структури якого увійшло Управління «К». Сьогодні діяльність цього підрозділу направлена на припинення найрізноманітніших видів протиправних діянь, і, в першу чергу, злочинів у сфері інформаційних технологій – таких як злочини у сфері комп'ютерної інформації, електронне шахрайство і т.ін.

У Сполучених штатах Америки питаннями боротьби зі злочинами у сфері високих технологій займаються декілька спеціальних державних організацій.

По-перше, це Федеральне бюро розслідування (the Federal Bureau of Investigation – FBI), у складі якого у 1996 році створено Кіберпідрозділ (Cyber Division FBI). Даний підрозділ функціонує на правах окремого управління в структурі ФБР та має чотири відділи, один з яких саме й займається питаннями протидії шахрайствам (Fraud) [1, 115].

Крім того, у складі Міністерства фінансів США діє Секретна служба США (US Secret Service), яка проводить розслідування фінансових злочинів за трьома напрямами:

– злочини проти фінансової системи (злочини проти фінансових установ (банківське шахрайство), шахрайство з використанням електронних засобів доступу (кредитних карток), відмивання грошей);

– злочини з використанням електронної апаратури (комп'ютерне шахрайство, шахрайство проти телефонних компаній);

– шахрайства проти державних фінансових програм (зобов'язання казначейства США, махінації з електронним переказом грошових коштів, інші махінації) [1, 116].

У Великобританії у 2001 році за ініціативою асоціації начальників поліції (ACPO) було створено Національний підрозділ по боротьбі зі злочинами у сфері високих технологій Королівства Великобританії (National High-Tech Crime Unit – NHTCU).

NHTCU займався розслідуванням таких злочинів, що скоюються у мережі Інтернет, як злами, віруси-хробаки, інтернет-шахрайства та інших злочинів у сфері високих технологій, пов'язаних із використанням комп'ютерів та телекомунікаційного обладнання [2].

1 квітня 2006 року у Великобританії на підставі Закону 2005 року «Про серйозну організовану злочинність та поліцію» (The Serious Organised Crime and Police Act 2005) [3] було створено Національне Агентство по боротьбі з організованою злочинністю (Serious Organised Crime Agency – SOCA) шляхом передачі функцій відділів та управлінь декількох правоохоронних органів Великобританії: Національної антикримінальної бригади (National Crime Squad – NCS), Національного підрозділу по боротьбі зі злочинами у сфері високих технологій (The National Hi-Tech Crime Unit – NHTCU), Національної служби кримінальної розвідки (National Criminal Intelligence Service), секції з розкриття та розслідування злочинів у сфері незаконного обігу наркотиків Королівської акцизної і таможеної служби (HM Revenue & Customs – HMRC), Митної служби в частині компетенції протидії організованій злочинності у сфері міграції. У 2008 році до SOCA приєдналося Агентство з вилучення активів (Assets Recovery Agency), у той же час як відділ по боротьбі з великим шахрайством (Serious Fraud Office) залишається окремим підрозділом.

На сьогоднішній день SOCA (як аналог Федерального бюро розслідування США) є самостійним (організаційно незалежним) міжвідомчим державним правоохоронним органом уряду Об'єднаного Королівства, що формально віднесений до Міністерства внутрішніх справ, який здійснює свою діяльність у межах всього Об'єднаного Королівства та співробітничає (через його мережу міжнародних представництв) з багатьма зарубіжними правоохоронними органами та спецслужбами [4].

У червні 2011 року коаліційний уряд Великобританії оголосив, що з 1 жовтня 2013 року функції SOCA в частині боротьби із комп'ютерною злочинністю будуть передані Національному підрозділу протистояння кіберзлочинам (National Cyber Crime Unit, NCCU) Національного агентства по боротьбі зі злочинністю (National Crime Agency, NCA) на підставі р.1 так званого "Білля про злочини й суди" Великобританії (The Crime and Courts Bill 2012-2013).

Важлива роль по протидії шахрайству у Великобританії відводиться також спеціальному управлінню Королівської прокурорської служби (Crown Prosecution Service – CPS), а саме – Центральній групі з протидії шахрайству, спеціалісти якої фокусують свої зусилля на підтриманні обвинувачення по справах про великі й складні шахрайства [5].

У 1994 році у складі поліцейського управління м.Мюнхен (Німеччина) було створено спеціальну групу по боротьбі зі злочинами у сфері високих технологій (AG EDV). Пізніше у

структурі федеральної поліції Німеччини створено групу «Технології», до складу якої входить понад 60 працівників кримінальної поліції, техніків, інженерів та вчених різних спеціальностей. Їх завданнями є як самостійне розслідування високотехнічних злочинів (у тому числі і шахрайств), так і сприяння роботі інших підрозділів, проведення досліджень і створення нових програмно-апаратних засобів для поліції, міжнародне співробітництво [1, 118].

У Французькій Республіці у 1994 році було створено «Службу по протидії зловживанням у сфері інформаційних технологій (SEFTI). Даний підрозділ підпорядковується Управлінню паризької кримінальної поліції, його компетенцією є боротьба з «інтелектуальним» піратством та «хакінгом». Розкриттям економічних злочинів у мережі Інтернет займається відділ Економічних та фінансових справ кримінальної поліції (SDAEF), а також спеціальна бригада по платіжним шахрайствам (BFMP), головним завданням якої є виявлення злочинів, пов'язаних з використанням платіжних карток [1, 118].

У Канаді функції боротьби з комп'ютерною злочинністю покладені на відділ економічних злочинів (CCS) Королівської канадської поліції, представництва якого створені в усіх великих містах країни (до складу представництва входить як мінімум один працівник – спеціаліст по розслідуванню комп'ютерних злочинів) та Відділ по високотехнічним злочинам (High Tech Crime Forensics Unit, HTCFU), який розміщено у головному офісі Королівської поліції в Оттаві [1, 122].

В Індії боротьбу з електронною злочинністю здійснює Центральне бюро розслідувань (Central Bureau of Investigation, CBI), у структурі якого з 2000 року функціонують сектор розслідування електронних злочинів та відділ з дослідження кіберзлочинності (Cyber Crime Research & Development Unit, CCRDU. Відділ CCRDU займається збиранням, накопиченням та аналізом інформації про комп'ютерні злочини [1, 123].

Стосовно другої групи спеціальних організацій, то тут ми можемо зазначити наступне: на сьогоднішній день у світі створено багато спеціальних організацій та експертних груп, що займаються вивченням комп'ютерних інцидентів та реєстрацією скарг на злочинні дії Інтернет спрямування, які виступають своєрідним «містком» між користувачами Інтернет та спеціальними державними організаціями, що займаються питаннями боротьби із комп'ютерними злочинами взагалі, та інтернет-шахрайством зокрема.

Одним із провідних центрів у світі, безперечно, є Центр по скаргах у мережі Інтернет (Internet Crime Complaint Center – IC3), який розташовується в Сполучених штатах Америки та координує роботу державних агентств, отримуючи та досліджуючи скарги на шахрайські та підозрілі дії в Інтернет-просторі з подальшим перенаправленням цієї інформації федеральним, державним, місцевим та міжнародним правоохоронним органам для вирішення питання про порушення кримінальних справ та кримінальне переслідування осіб, що вчинили злочинні дії у мережі Інтернет.

IC3 діє у тісній співпраці з Центром дослідження біловоротничкової злочинності (National White Collar Crime Center – NW3C), з Федеральним бюро розслідування (the Federal Bureau of Investigation – FBI) та з Бюро юридичної допомоги департаменту Юстиції США (Bureau of Justice Assistance – BJA) [6].

Окрім IC3, ми можемо назвати три основних види експертних груп, що існують у світі, які займаються вивченням інцидентів в комп'ютерній та інтернет-безпеці, а саме:

1) комп'ютерні групи реагування на надзвичайні ситуації (Computer Emergency Response Team, CERT);

2) команди комп'ютерної безпеки по реагуванню на інциденти (Computer Security Incident Response Team, CSIRT);

3) комп'ютерні команди екстреної готовності (Computer Emergency Readiness Team).

Крім того, в світі вже створені міжнародні об'єднання CSIRT/CERT центрів, такі як Forum of Incident Response and Security Teams (FIRST) – Коаліція центрів реагування на комп'ютерні інциденти; та Trusted Introducer – співтовариство, що об'єднує європейські команди реагування на інциденти інформаційної безпеки.

Перший координаційний центр CERT (CERT Coordination Center, CERT/CC) було створено у листопаді 1988 року в Інституті програмного забезпечення та технічних наук (SEI) Університету Карнегі-Меллона (м. Піттсбург, США), після того як так званий «хробак Морриса» уразив комп'ютери Агентства з перспективних оборонних науково-дослідних розробок Міністерства оборони США (Defense Advanced Research Projects Agency – DARPA) [7].

Окрім CERT/CC в США у вересні 2003 року було створено Групу готовності до надзвичайних ситуацій в інформаційних системах США (United States Computer Emergency Readiness Team, US-CERT). US-CERT є частиною Національного відділу кіберзахисту Міністерства національної безпеки США (the Department of Homeland Security). US-CERT є центральним цілодобово функціонуючим органом, відповідальним за взаємодію з урядовими структурами (як федеральними, так і місцевими), а також іншими суб'єктами з питань захисту інформації. Її основним обов'язком є збір і поширення інформації з метою реагування на інциденти, підвищення рівня скоординованості дій, зниження рівня уразливості. Крім того, US-CERT займається розповсюдженням інформації про поточні питання безпеки, уразливості та експлойти через National Cyber Alert System та працює з постачальниками програмного забезпечення для створення патчей, що усувають уразливості в системах безпеки. US-CERT перебуває у складі Федерального центру керування інцидентами уряду США й виступає координатором з питань комп'ютерної безпеки США [8].

В Російській Федерації на сьогоднішній день також діє декілька аналогічних таких центрів – RU-CERT, CERT-GIB, WebPlus ISP, GOV-CERT.RU.

RU.CERT (Russian Computer Emergency Response Team) – це автономна некомерційна організація "Центр реагирования на компьютерные инциденты" (створена у 1998 році), яка офіційно зареєстрована як Computer Security Incident Response Team (CSIRT) і входить до складу міжнародних об'єднань CSIRT/CERT центрів (таких як FIRST та Trusted Introducer), та офіційно, в рамках даних об'єднань, виконує функції контактної сторони в Російській Федерації.

Основне завдання центру – зниження рівня загроз інформаційної безпеки для користувачів російського сегменту мережі Інтернет. RU-CERT здійснює збір, зберігання й обробку статистичних даних, пов'язаних з поширенням шкідливих програм і мережних атак на території РФ, сприяючи таким чином російським та закордонним юридичним і фізичним особам при виявленні, попередженні й припиненні протиправної діяльності, яка має відношення до розташованих на території Російської Федерації мережних ресурсів.

Для реалізації поставлених завдань RU-CERT взаємодіє із провідними російськими IT компаніями, суб'єктами оперативно-розшукової діяльності, органами державної влади та управління, закордонними центрами реагування на комп'ютерні інциденти та іншими організаціями, що здійснюють свою діяльність в області комп'ютерної та інформаційної безпеки.

Слід зазначити, що, діючи в рамках нормативно-правової бази РФ, RU-CERT не уповноважений займатися вирішенням питань, що перебувають у веденні правоохоронних органів. В цих випадках необхідно звертатися в регіональні підрозділи ФСБ або МВС РФ [9].

CERT-GIB було створено у 2012 році компанією Group-IB. CERT-GIB – це приватний центр реагування, що обслуговує сторонні організації, але, претендує на звання "продержавного", тому що саме з ним Координаційний центр російського домена мережі Інтернет уклав угоду про протидію кіберзагрозам у доменах .RU і .РФ (поряд з підрозділом Ліги безпечного Інтернету – фондом "Дружній Рунет"). Центр працює в режимі 24x7 і надає послуги (на підставі абонентського договору або договору оферти) реагування на наступні типи інцидентів: відмова в обслуговуванні (Dos, DDos), компрометація інформації, компрометація активу, внутрішній або зовнішній несанкціонований доступ, створення й поширення шкідливого програмного забезпечення, порушення політики інформаційної безпеки, фішинг і незаконне використання бренда в Інтернеті, шахрайські дії із системами ДБО та електронними платіжними системами [10].

Необхідно зазначити, що Group-IB (компанія – засновник CERT-GIB) – одна із провідних міжнародних компаній по запобіганню й розслідуванню кіберзлочинів та шахрайств із використанням високих технологій, основними напрямками діяльності якої є моніторинг і

запобігання кіберзагроз; аудит інформаційної безпеки; комп'ютерна криміналістика; розслідування кіберзлочинів і шахрайств із використанням високих технологій; розробка інноваційних програмних продуктів щодо моніторингу, виявлення та запобігання виникаючих кіберзагроз [11].

Нещодавно в РФ було створено ще один центр – GOV-CERT.RU – центр реагування на комп'ютерні інциденти в інформаційно-телекомунікаційних мережах (ІТМ) органів державної влади РФ, покликаний вирішувати наступні завдання: надання консультативної та методичної допомоги при проведенні заходів щодо ліквідації наслідків комп'ютерних інцидентів в ІТМ органів державної влади; аналіз причин і умов виникнення інцидентів в ІТМ органів державної влади; вироблення рекомендацій зі способів нейтралізації актуальних загроз безпеки інформації; взаємодія з російськими, іноземними й міжнародними організаціями, відповідальними за реагування на комп'ютерні інциденти; нагромадження й аналіз відомостей про такі інциденти [12].

Центр Webplus ISP CERT займається обслуговуванням тільки власних ресурсів.

Окрім зазначених центрів, в Російській Федерації діє ще Національний центр по боротьбі зі злочинами у сфері високих технологій (National Hi-Tech Crime Unit.ru). Національний центр по боротьбі зі злочинами у сфері високих технологій – це недержавна міжвідомча організація, що проводить незалежні комп'ютерні, комп'ютерно-технічні та інші види експертиз і досліджень на замовлення експертно-криміналістичних підрозділів Міністерства внутрішніх справ (МВС) РФ та Міністерства юстиції РФ (зокрема, Російського федерального центру судової експертизи (РФЦСЕ) Міністерства юстиції РФ), Слідчого комітету при МВС РФ, деяких регіональних та районних відділів і управлінь Федеральної служби безпеки (ФСБ) РФ, МВС РФ, прокуратур та регіональних слідчих комітетів при Прокуратурі РФ, і т.ін. [13].

Крім того, на сьогоднішній день в Російській Федерації ще створюється також міжгалузевий CSIRT (Computer Security Incident Response Team) на базі Асоціації керівників служб інформаційної безпеки.

У ЄС більшість груп CERT були локально створені університетами й великими ІТ-компаніями. Більшість країн-членів ЄС не мають національного координаційного центру та співпрацюють через загальноєвропейський TF-CSIRT (Task Force – Collaboration Security Incident Response Teams). Саме TF-CSIRT запустив FIRST (Forum of Incident Response and Security Teams – Коаліція центрів реагування на комп'ютерні інциденти) для нарад з питань команд CERT. Керування центрами CERT ЄС поступово передається агентству ENISA.

Так, у Німеччині ми можемо назвати декілька таких CERT-центрів: RUS CERT (www.cert.uni-stuttgart.de), DFN CERT (www.cert.dfn.de), CERT-Bund (www.bsi.de/certbund), Bürger-CERT (www.buerger-cert.de), CERT-Verbund (www.cert-verbund.de), Siemens-CERT (www.siemens.com/cert), S-CERT (www.s-cert.de).

У Франції діють такі центри, як CERTA (www.certa.ssi.gouv.fr), Cert-IST (www.cert-ist.com) та CERT-RENATER (www.renater.fr/spip.php?rubrique19); в Італії – CERT GARR (www.cert.garr.it); у Швейцарії та Ліхтенштейні – SWITCH CERT (www.switch.ch/cert); в Австрії – CERT.at (www.cert.at) та ACOnet CERT (www.cert.aco.net).

Стосовно діяльності міждержавних організацій ми можемо зазначити, що, наприклад, у 2001 році Всесвітнім банком було створено Департамент по боротьбі із шахрайством, корупцією та корпоративними порушеннями (INT), який займається розслідуваннями в рамках Групи організацій Всесвітнього банку та прямо підзвітний Президенту, а побічно – Ревізійному комітету Ради виконавчих директорів Групи організацій Всесвітнього банку. INT направляє Президенту свої доповіді за результатами розслідувань і щоквартально звітує перед Ревізійним комітетом за підсумками проведення важливих заходів і результатами діяльності підрозділу. У 2008 фінансовому році INT одержав статус управління, очолюваного віце-президентом [14].

Таким чином, досвід провідних країн світу щодо збирання, дослідження та обміну інформацією про комп'ютерні інциденти та кіберзагрози цілком можна використовувати і в Україні шляхом створення Бази данних інтернет-інцидентів та Центру скарг Інтернет-злочинності за аналогією із IC3 (Internet Crime Complaint Center – США) та RU CERT (Центр реагування на комп'ютерні інциденти Російської Федерації) та ін.

ЛІТЕРАТУРА

1. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток: науково-практичний посібник / В.М. Бутузов, В.Д. Гавловський, К.В. Тітуніна, В.П. Шоломенцев; за ред. І.В. Бондаренка. – К.: ТОВ «Видавничий будинок «Аванпост-Прим», 2009. – 182 с.
2. National High-Tech Crime Unit – NHTCU [Electronic resource]. – Mode of access: http://en.wikipedia.org/wiki/National_Hi-Tech_Crime_Unit
3. The Serious Organised Crime and Police Act 2005 [Electronic resource]. – Mode of access: http: www.legislation.gov.uk.
4. Serious_Organised_Crime_Agency – SOKA [Electronic resource]. – Mode of access: http://en.wikipedia.org/wiki/Serious_Organised_Crime_Agency
5. Клейменов И.М. Борьба с организованной преступностью в Великобритании [Электронный ресурс] / И.М. Клейменов. – Режим доступа: http://justicemaker.ru/view-article.php?id=15&art=3375
6. The Internet Crime Complaint Center (IC3) [Electronic resource]. – Mode of access: http://www.ic3.gov
7. CERT Coordination Center (CERT/CC) [Electronic resource]. – Mode of access: http://www.cert.org/certcc.html
8. United States Computer Emergency Readiness Team (US-CERT) [Electronic resource]. – Mode of access: http://www.us-cert.gov/
9. Центр реагирования на компьютерные инциденты Российской Федерации RU-CERT [Электронный ресурс]. – Режим доступа: http://www.cert.ru.
10. Центр круглосуточного реагирования на инциденты информационной безопасности CERT-GIB [Электронный ресурс]. – Режим доступа: http://www.cert-gib.ru.
11. Компания Group-IB [Электронный ресурс]. – Режим доступа: http://www.group-ib.ru/index.php/o-kompanii/15-o-group-ib
12. Центр реагирования на компьютерные инциденты в информационно-телекоммуникационных системах органов государственной власти Российской Федерации GOV-CERT.RU [Электронный ресурс]. – Режим доступа: http://www.gov-cert.ru.
13. Национальный центр по борьбе с преступлениями в сфере высоких технологий (National Hi-Tech Crime Unit.ru) [Электронный ресурс]. – Режим доступа: http://www.nhtcu.ru/
14. Ежегодный доклад управления по борьбе с мошенничеством, коррупцией и корпоративными нарушениями группы организаций Всемирного банка [Электронный ресурс]. – Режим доступа: http://siteresources.worldbank.org/

УДК 343. 1 (477)

ПОНЯТТЯ ТА ПРОЦЕСУАЛЬНИЙ ПОРЯДОК ЗНЯТТЯ СУДИМОСТІ: ПРОБЛЕМНІ ПИТАННЯ

Дільна З.Ф., аспірантка

Львівський національний університет ім. Івана Франка

У статті досліджено поняття правової природи інституту зняття судимості. Розглянуто актуальні питання, що стосуються процесуального порядку та діяльності суду з вирішення питання про зняття