УДК 351.74

Олексій Олександрович Деревягін
кандидат юридичних наук, старший науковий співробітник,
доцент кафедри оперативно-розшукової діяльності та розкриття злочинів
факультету № 2 Харківського національного університету внутрішніх справ

Протидія кіберзлочинності в Україні, як складова забезпечення міжнародної безпеки

Питання пошуку шляхів протидії злочинам з використанням інформаційно-комунікаційних систем уже тривалий час знаходиться у сфері уваги як державних правоохоронних органів, так й міжнародної спільноти. Беручи до уваги, що розвиток інформаційних технологій йде швидше ніж приймаються нормативно-правові акти, якими вони регулюються, а об'єми незаконно одержаних коштів кіберзлочинцями зростають, необхідно на постійній основі знаходити шляхи вирішення нових задач, пов'язаних з такими сферами, як захист даних, транскордонний доступ правоохоронних служб до даних та обмін інформацією між державними та приватними структурами тощо.

Цілком зрозуміло, що міжнародні організації виказують стурбованість з цього приводу та відзначають необхідність скоординованої міждержавної взаємодії при розслідуванні кіберзлочинів. Саме завдяки роботі таких міжнародних організацій, як Організація економічного співробітництва і розвитку (далі – ОЕСР), Інтерпол, Група Восьми (далі – G8), Рада Європи, ООН, розвивається міжнародна співпраця країн у сфері протидії кіберзлочинності, формується міжнародне законодавство. Проте для розробки і впровадження міжнародно-правових норм в національне законодавство вкрай необхідно сформулювати єдиний підхід до розуміння, як єдиних завдань,

вироблення загальних принципів, так і визначення пріоритетних напрямів вирішення наявних проблем.

Неузгоджений підхід у кримінальному законодавстві різних держав до формулювання конкретних складів злочинів не сприяє ефективній протидії комп'ютерним злочинам у глобальному масштабі. У зв'язку з цим міжнародно-правове регулювання повинне відігравати головну роль в гармонізації національного кримінального законодавства з міжнародно-правовими актами, розробленими і прийнятими відповідними організаціями.

Крім того, з метою реалізації ефективних заходів протидії кіберзлочинності підрозділами боротьби з кіберзлочинністю Національної поліції України важливо враховувати позитивний досвід правоохоронних органів зарубіжних країн. Так, наприклад, національні законодавства і правоохоронні органи різних країн у своїй діяльності вимушені брати до уваги особливості кордонів, мовні, політичні, релігійні особливості, що впливають на ефективність протидії злочинності в досліджуваній сфері.

Специфічність характеристик вимагає міждержавного підходу до протидії кіберзлочинам, ефективність якого недосяжна без міжнародної співпраці. Необхідно також звернути увагу на те, що досвід розвинених зарубіжних країн говорить про неухильне збільшення із року в рік кількості служб і відомств в сфері протидії кіберзлочинності, тому варто систематично вивчати і переймати їх досвід. Наприклад, у США створені такі відомства, як Electronic Crimes Task Forces ECTF, підрозділ Секретна служба США (United States Secret Service USSS). Ці підрозділи створюють взаємодію між службами, правоохоронними органами (федерального рівня, рівня штату, локальними), приватним сектором, академічним співтовариством і виявляють і запобігають кіберзлочинам.

У Великій Британії боротьбою з кіберзлочинністю займається відділ по боротьбі з кіберзлочинами, що входить до складу Агентства по боротьбі з організованою злочинністю. У ФРН основну діяльність щодо боротьби з кіберзлочинністю здійснює Федеральна кримінальна поліція. У Франції 1 липня 2008 р. шляхом об'єднання двох спецслужб Центрального директорату

загальної розвідки (RG) і Директорату стеження за територіями (DST) створено Головне управління внутрішньої розвідки Direction centrale du Renseignement interieur, DCRI.

В Естонії в 2006 р. створено комп'ютерну групу реагування на надзвичайні ситуації (CERT-EE). У Республіці Білорусь Управління по розкриттю злочинів у сфері високих технологій Міністерства внутрішніх справ є самостійним оперативно-розшуковим підрозділом Міністерства, безпосередньо підпорядкованим першому заступникові Міністра внутрішніх справ – начальникові головного управління кримінальної міліції [1].

Власну стратегію щодо вирішення проблем протидії кіберзлочинності розроблено також Європейським поліцейським відомством (Європол). На даний час Європол надає членам ЄС слідчу і аналітичну підтримку через свою систему онлайн-розслідувань і базу даних злочинів. З січня 2013 року під егідою Європолу розпочав діяльність новий Європейський центр боротьби з кіберзлочинністю. Серед пріоритетів Центру – розслідування шахрайства через онлайн-мережі, зокрема у системі електронного банкінгу та інших видах фінансової діяльності, протидія сексуальній експлуатації дітей через Інтернет, а також розслідування інших злочинів, що посягають на безпеку важливої інфраструктури та інформаційних систем ЄС.

Перераховані вище обставини обумовлюють прийняття спеціального законодавства та розробки загальнодержавної комплексної стратегії протидії кіберзлочинності в Україні із урахуванням європейського досвіду, а також визначення основних напрямів діяльності державних органів та органів місцевого самоврядування, інститутів громадянського суспільства, юридичних і фізичних осіб щодо захисту основ конституційного устрою, прав і свобод людини та громадянина, забезпечення цілісності й національної безпеки держави, виявлення і ліквідації причин та умов, що сприяють проявам кіберзлочинності.

З урахуванням зазначених пропозицій та рекомендацій протидія кіберзлочинності в України буде відповідати міжнародним стандартам, що

сприятиме покращенню правоохоронної діяльності у сфері інформаційної та економічної безпеки України в цілому.

Список використаних джерел:

1. Интерпол: Киберпреступления являются самой опасной криминальной угрозой: [электронный ресурс]. – Режим доступа: http: //www.virusovnet.org/main/309.

Одержано _____