СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
ЛІГА СТУДЕНТІВ АСОЦІАЦІЇ ПРАВНИКІВ УКРАЇНИ

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
IV Міжнародної науково-практичної конференції
(Суми, 21–22 травня 2020 року)

У двох частинах

Частина 2

Суми
Сумський державний університет
2020

ЛІТЕРАТУРА:

1. Конституція України від 28 червня 1996 року. Дата оновлення: 01.01.2020 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 25.03.2020).
2. Про внесення змін до деяких законодавчих актів України щодо забезпечення особистого голосування народними депутатами України на пленарних засіданнях Верховної Ради України: Закон України від 19 грудня 2019 року № 404-IX. URL: https://zakon.rada.gov.ua/laws/show/404-20#n6 (дата звернення: 25.03.2020).
3. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. Дата оновлення: 20.03.2020 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 25.03.2020).
4. Про статус народного депутата України : Закон України від 17 листопада 1992 року № 2790-XII. Дата оновлення: 20.03.20 р. URL: https://zakon.rada.gov.ua/laws/show/2790-12 (дата звернення: 25.03.2020).

БОРОТЬБА З КІБЕРЗЛОЧИНАМИ: ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ МІЖНАРОДНОГО ДОСВІДУ В УКРАЇНІ

Хуторянець Ж. В.
Студентка III курсу ННІ права
Сумського державного університету
Науковий керівник: Думчиков М. О.
к. ю. н., асистент кафедри КПДС ННІ права
Сумського державного університету

Законодавство України у сфері боротьби з кіберзлочинністю нині є ще недосконалим та потребує уніфікації з урахуванням результатів випереджувальної еволюції країн-лідерів, їх досягнень та міжнародного досвіду, а також запиту суспільства на зміни.

Разом з тим, тенденції до поширення й масштаби кіберзлочинності та її соціально небезпечні наслідки викликають серйозне занепокоєння міжнародного співтовариства, спонукаючи до вдосконалення, трансформації норм, що регулюють норм, що регулюють суспільні відносини в кіберпросторі.

Аналіз національного законодавства України з питань запобігання кіберзлочинності й вчинення кібершахрайства дозволяє стверджувати про те, що законодавець певною мірою визначив основні поняття, запобіжні заходи з профілактики та протидії злочинності в кіберпросторі.

Водночас законодавство повинно корелювати з сучасним рівнем розвитку технологій, а пріоритетом є організація взаємодії і координація зусиль правоохоронних оргнаів, спецслужб, судової системи, їх інформаційне та ресурсне забезпечення [1].

На нашу думку, міжнародний досвід використання засобів запобігання кібершахрайству, юриздикції суб'єктів такої діяльності на прикладах окремих країн.

Так, О. А. Баранов констатує, що США, гостро відчуваючи проблему кіберзлочинності, намагаються побудувати розгалужену систему боротьби з нею [2]. У ФБР створено Центр кіберзлочинів і оцінки загрози інфраструктурі, який отримав широкі повноваження з контролю за найбільш чутливими складовими інформаційної інфраструктури держави: фінансовою системою, телефонною мережею, управлінням рухом, управлінням енергосистемою тощо.

У Федеративній Республіці Німеччина (ФРН) боротьбу з кіберзлочинністю здійснює: Федеральна кримінальна поліція, Національний центр по боротьбі з кіберзлочинністю при Федеральному агентстві з інформаційних технологій, головним завданням якого є координація діяльності державних органів у боротьбі з кіберзлочинністю та використанням новітніх технологій у боротьбі з кібератаками [3]. З метою координації профілактичної діяльності в багатьох країнах створені відповідні органи – національні ради, основними функціями яких є:

– збір інформації, планування, виконання та оцінка програм профілактики злочинів;

– координація діяльності поліції та інших органів, що працюють у цій сфері, забезпечення участі населення, співробітництво зі ЗМІ;

– науково-дослідна робота, навчальна підготовка тощо.

Поліція ФРН запровадила адресну роботу превентивного характеру із громадськістю, орієнтовану на самозахист, що здійснюється шляхом безкоштовних консультацій населення, як за допомогою технічних засобів уберегти від злочинців майно, не стати жертвою злочину [4].

У США використовуються такі моделі превентивної діяльності: громадських установ, безпеки індивідуума та впливу через навколишнє середовище.

У Канаді широко використовується участь громадян у превенції злочинів знижуючи страх перед злочинцями, підтримуючи відчуття особистої безпеки.

Уся ця діяльність дістає моральну й матеріальну підтримку суспільства й держави [5, с. 60-61]. Слід підкреслити, що в цьому випадку частина культурно-виховних запобіжних заходів здійснюється саме правоохоронними органам, котрі активно взаємодіють з громадянами, що без сумніву позитивно впливає на зниження показників

злочинності, а також на рівень довіри суспільства до результатів правоохоронної діяльності.

У Великій Британії боротьбу з кіберзлочинністю здійснюють відділ по боротьбі з кіберзлочинами, що входитьдо складу Агентства по боротьбі з організованою злочинністю, який взаємодіє з відповідними підрозділами ФБР, а також Поліцейський національний відділ по боротьбі зі злочинами у сфері високих технологій з координуючими функціями [3].

Варто зазначити найбільш конструктивні запобіжні профілактичні засоби, котрі ефективно використовує міжнародне співтовариство.

Так, у країнах ЄС виділяють два рівні профілактики злочинів: соціальний і ситуаційний. Соціальна профілактика спрямована на зміну несприятливих умов формування особистості людини, особливо мікросередовища й мікросоціальної ситуації. Ситуаційна виходить із того, що окремі категорії кіберзлочинів учиняються за певних обставин, у певний час і певних місцях.

У ФРН виділяють первинну, вторинну і третинну превенцію. Первинну спрямовано на подолання дефіциту соціальності й позитивної правосвідомості як головної причини злочинів. Вторинна здійснюється поліцейськими органами й пов’язанаіз правовими засобами втримання від учинення злочинів. Третинна превенція – це ті профілактичні заходи й засоби, що застосовуються у процесі покарання та ресоціалізації злочинців [5, с. 60, 61]. Отже, профілактика кіберзлочинів починається з використанням організаційно-виховних запобіжних заходів. На наш погляд, вдалим є приклад ФРН, котрий демонструє взаємодіюгромадян із патрульними, що є одним із засобів ситуативної профілактики злочинів.

Також слід удосконалити взаємодію правоохоронних органів з іншими державними органами. Наприклад, відповідно до Конвенції Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов’язана з протидією злочинності, плануєтьсястворити систему, що сприятиме істотному вдосконаленню інформаційної взаємодії правоохоронних та інших державних органів у сфері протидії злочинності, поліпшенню координації їх діяльності, забезпеченню спільного формування та використання інформаційних ресурсів для ефективної протидії злочинності, здійсненню аналітичної, статичної та управлінської діяльності у сфері захисту конституційних прав та свобод людини і громадянина від злочинних проявів як найбільш небезпечної загрози державній безпеці України [4].

Саме тому перспективними напрямами розвитку інформаційних технологій суб’єктів боротьби з кіберзлочинністю взагалі та кібершахрайствомзокрема є:

– створення єдиного інформаційно-аналітичного комплексу як інтегрованої системи інформаційних ресурсів підтримкиоперативно-службової діяльності, підвищення спроможностей з протидії кіберзлочинності;

– розробка автоматизованої системи проведення оперативно-розшукових заходів у телекомунікаційних мережах загального користування з автоматизованим проведенням окремихоперативно-технічних заходів та негласних слідчих (розшукових) дій;

– розвиток ідеї використання автоматизованих робочих місць спеціаліста (криміналіста, слідчого, детектива, дільничного тощо), що інтегрується до інформаційної системи;

– впровадження дистанційної системи підготовки та перепідготовкиперсоналу [6, с. 159-160].

З огляду на позитивний зарубіжний досвід, доцільно вдосконалювати заходи запобігання кібершахрайству шляхом:

– упровадження профілактичних засобів запобігання кіберзлочинності та кібершахрайству за рахунок ситуативної профілактики у вигляді організації співпраці з поліції з громадянами;

– формування та врегулювання програмних документів щодо взаємодії правоохоронних органів та інших державних органів у сфері протидії кіберзлочинності щляхом створення автоматизованої інтегрованої інформаційної системи, що включатиме аналітичні, статистичні ресурси, пошукові системи, бази даних про злочинців та правопорушників;

– створення єдиного комплексу заходів на основі міжнародної взаємодопомоги в розслідуванні кіберзлочинів, виявлені, закріплені та вилученні комп’ютерної інформації, її передачі іншій державі, а також у наданні сприяння при проведенні транскордонного обшуку в комп’ютерних мережах, з метою використання в кримінальному судочинстві як доказів після відповідного документування і копіювання комп’ютерної інформації [7, с. 289].

Виходячи із вищезазначеного можна зробити висновок, що ефективна протидія кібершахрайству можливо лише за умови узгодженої взаємодії та єдності, реалізації спільної кримінальної політики, удосконалення законодавства, налагодження міжнародного співробітництва, оскільки актуальність запобігання кібезлочинам залишається незмінною, а дослідження цього питання – доречним зараз та буде перспективним у майбутному.

ЛІТЕРАТУРА:

1. Кіберзлочинність в Україні. Соціальна мережа науковців. URL: http://www.science-community.org/uk/node/16132.
2. Баранов О. А. Кримінологічні проблеми комп'ютерної злочинності. URL: http://www.bezpeka.com/ru/lib/spec/crim/art71.html.
3. Манжай О.В. Досвіб Великобританії, ФРН та КНР. Навчально-тренувальний центр боротьби з кіберзлочинністю та моніторингу кіберпростору на громадських засадах. Офіційний веб-сайт. URL: http://cybercop.in.ua/index.php/naukovi-statti/80naukovi-statti/201-dosvid-velikobritaniji-frn-t-knr.
4. Шапочка С. В. Міжнародні стандарти з кібербезпеки та досвід боротьби з кіберзлочинністю і кібершахрайством. *Наука і правоохорона*. 2017. № 3 (37). С. 177–184.
5. Миронюк Т. В. превентивна та віктимологічна профілактика міжнародний аспект. Віктимологічна профілактика окремих видів злочинів: тези доповідей круглого столу (Київ, 29 квітня 2014 року); ред. кол. О. М. Джужа, В. В. Василевич, Т. Л. Кальченко та ін. Київ: Нац. акад. внутр. справ, 2014. 215 с.
6. Безруков Д. В. Інформаційні технології в діяльності органів внутрішніх справ: поняття, напрямки використання, перспектива. Протидія злочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., м. Харків, 23 квіт. 2013 р., МВС України, Харк. нац. ун-т внутр. справ; Незалеж. асоц. Банків України, Харк. Банк. Союз регіон. представник НАБУ. Харків; ХНУВС, 2013. 286 с.
7. Волеводз А. Г. Противодействие киберпреступлениям: правовые основы международного сотрудничества. Москва: ООО «Издательство «Юрлитинформ», 2001. 496 с.

ЛЕГАЛІЗАЦІЯ ГРАЛЬНОГО БІЗНЕСУ ЯК СПОСІБ ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЯ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Білик Г. В.
Студентка ІІІ курсу ННІ права
Сумського державного університету
Науковий керівник: Бондаренко О. С.
к. ю. н., старший викладач кафедри КПДС ННІ права
Сумського державного університету

На сьогодні, гральний бізнес в Україні є забороненим згідно з Законом України «Про заборону грального бізнесу в Україні». Однак, починаючи з минулого року розпочався активний процес легалізації даного виду бізнесу. Перші читання нового