

Список бібліографічних посилань

1. Конституція України : закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Про затвердження Інструкції про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної, холодної і охолощеної зброї, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями металевими снарядами не смертельної дії, та патронів до них, а також боєприпасів до зброї, основних частин зброї та вибухових матеріалів : наказ МВС України від 21.08.1998 № 622 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/z0637-98> (дата звернення: 01.03.2019).
3. Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.
4. Фріс П. Л. Право громадян на зброю – «PRO ET CONTRA». *Наше право*. 2015. № 5. С. 77–84
5. Цивільна зброя в Україні: міфи та реальність. Українська дійсність і міжнародний досвід легалізації та контролю / Г. Ф. Гергеа, О. О. Зарубінський, Б. М. Петренко, Р. В. Старовойтенко. Київ : АДЕФ-Україна, 2015. 152 с.
6. Гергеа Г. Ф., Зарубінський О. О., Петренко Б. М., Старовойтенко Р. В. Цивільна зброя в Україні: міфи та реальність. Українська дійсність і міжнародний досвід легалізації та контролю. Київ : АДЕФ-Україна, 2015. 52 с.

Одержано 06.03.2019

УДК 343.32+343.346.8

Владислав Сергійович ГЕРАСИМЮК,

курсант 3 курсу факультету № 4

Харківського національного університету внутрішніх справ

Науковий керівник:

Ксенія Володимирівна ЮРТАЄВА,

кандидат юридичних наук,

доцент кафедри кримінального права і кримінології факультету № 1

Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЯК СКЛАДОВОЇ ПУБЛІЧНОЇ БЕЗПЕКИ

Останнім часом в умовах стрімкого розвитку інформаційних технологій і виникнення численних гібридних загроз проблема забезпечення публічної безпеки стає все більш складною. Згідно п. 4 ст. 3 закону України «Про національну безпеку України» державна політика у сферах національної безпеки і оборони охоплює низку різних напрямів і спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, в тому числі й кібербезпеки України [1]. Відповідно до ст. 1 закону України «Про основні засади забезпечення кібербезпеки України» кібербезпекою визнається захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [2]. Таким чином відповідно до чинного законодавства кібербезпека визнається важливою складовою публічної безпеки, і органи Національної поліції України є частиною національної системи кібербезпеки України (п. 3 Стратегії кібербезпеки України) [3].

На сьогодні жодна галузь людської діяльності не набула такого розвитку, як інформаційні технології. Інформаційні технології трансформують світ, розширюють особисту свободу і можливості людей, допомагають створювати нові ідеї та інновації. Проте разом із перевагами сучасного цифрового світу та розвитком інформаційних технологій також зростає і кількість загроз публічній безпеці, супроводжуваних зростанням кількості та потужності кібератак,

вмотивованих інтересами окремих держав, груп та індивідів. Переважна більшість Українців має низький рівень володіння комп'ютером, зазвичай навіть не помічаючи жодних змін від справжньої ліцензійної програми. Встановивши шкідливий софт потерпілий надає доступ злочвмисникам до персональних даних, що знаходяться на його комп'ютері, у тому числі інформації щодо номерів банківських карток, паролів до соціальних мереж та багато іншого включаючи особисте листування. Часто навіть не підозрюючи про витік комп'ютерної інформації потерпілі користуються такими софтами місяцями. Цим самим вони дають зловмисникам змогу заволодіти коштами з їх рахунків, або рахунків їх фірм чи організацій. І це лише один із прикладів кіберзлочинів, з якими щодня стикаються працівники Кіберполіції України.

Проаналізувавши дані, отримані в результаті інформаційного запиту, направлено нами до Генеральної прокуратури України, про статистику вчинення кіберзлочинів в Україні станом на 2018 рік [4], мусимо констатувати, що сучасний стан системи публічної безпеки не забезпечує у повному обсязі нейтралізацію існуючих кіберзагроз. Так, у 2018 р. в Україні зареєстровано – 2470 кримінальних правопорушень у сфері кіберзлочинності, із них закриті – 169, направлені до суду (з урахуванням правопорушень минулих років) – 1515. Аналізуючи статистику кіберзлочинів в областях України можна прийти до висновку, що найбільшу кількість зареєстрованих кіберзлочинів зафіксовано в таких областях як: Миколаївська – 378; Одеська – 351; Львівська – 272 та у місті Києві – 283 злочини. Найменша кількість кіберзлочинів зареєстровано в Івано-Франківській – 20; Тернопільській – 25; Волинській – 29 та Сумська – 30 злочинів.

Аналізуючи кримінологічні характеристики осіб, що вчинили кіберзлочини у 2018 р., можна прийти до наступних висновків: більшість осіб, що вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) у віці 29–39 років. З 254 облікованих, осіб, що вчинили зазначені злочини у 2018 р., 145 осіб мали повну вищу або базову вищу освіту, 66 осіб – вищу загальну середню або базову загальну середню освіту, 40 осіб – професійно технічну освіту, 3 особи – початкову базову або взагалі не мали освіти [4].

За словами голови Кіберполіції Сергія Демедюка щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисяч. У 2017 році підрозділи Кіберполіції супроводжували близько 7 тис. кримінальних проваджень, з них 4,5 тис – винятково кіберзлочини. За одинадцять місяців 2017 року було направлено до суду обвинувальні акти щодо 726 осіб [5]. Відповідно до отриманої нами статистики Генеральної Прокуратури України у 2018 кількість кримінальних проваджень, направлених до суду з обвинувальним актом зросла вдвічі і складає 1515 кримінальних справ [4], що свідчить про поліпшення роботи правоохоронних органів у напрямку протидії кіберзлочинам.

З кожним роком кількість вчинених кіберзлочинів зростає, способи їх вчинення постійно удосконалюється, що у свою чергу ускладнює виявлення та протидію зазначеним правопорушенням. Одними з першочергових заходів на шляху побудови системи кібербезпеки є вдосконалення державного управління у даній сфері та нормативно-правової бази для забезпечення такої діяльності. Крім того важливим є здійснення посиленої професійної підготовки, проведення курсів підвищення кваліфікації, тренінгів, з питань кібербезпеки і не лише для працівників Кіберполіції України, а й для усіх співробітників правоохоронних органів. Так, наприклад, підготовка суддів, слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів є одним із важливих заходів, передбачених Стратегією кібербезпеки України [3]. Крім того для підвищення поінформованості громадян про безпеку в кіберпросторі важливим є проведення превентивних заходів, лекцій у навчальних закладах, на підприємствах, організаціях, розміщення інформації у місцях найбільшої активності людей щодо безпечного користування всесвітньою мережею Інтернет. Реалізація комплексу зазначених заходів є необхідною умовою забезпечення публічної безпеки в нашій державі.

Список бібліографічних посилань

1. Про національну безпеку : закон України від 21.06.2018 № 2469-VIII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 26.01.2019).
2. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 26.01.2019).

3. Стратегія кібербезпеки України : затв. указом Президента України від 15.03.2016 № 96/2016 // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/96/2016> (дата звернення: 26.01.2019).

4. Статистика кіберзлочинності в Україні за 2018 рік // Доступ до правди : сайт. URL: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v_4?nocache=incoming-105671#incoming-105671 (дата звернення: 26.01.2019).

5. Кількість кіберзлочинів збільшується на 2,5 тисячі в рік – голова Кіберполіції // Економічна правда : сайт. URL: <https://www.epravda.com.ua/news/2018/01/15/633010/> (дата звернення: 26.01.2019).

Одержано 28.01.2019

УДК 343.9

Євгенія Олексіївна ГЛАДКОВА,

кандидат юридичних наук, старший дослідник,
старший науковий співробітник науково-дослідної лабораторії з проблем протидії злочинності
Харківського національного університету внутрішніх справ

РЕГІОНАЛЬНИЙ ВИМІР ЗАБЕЗПЕЧЕННЯ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ

Феномен кримінологічної безпеки безпосередньо пов'язаний із протидією злочинності – «системою державних і громадських заходів, спрямованих на усунення або нейтралізацію детермінант злочинності та корекцію поведінки осіб, схильних до правопорушень» [1]. Як особливий, інтегрований, багаторівневий об'єкт соціального управління протидія злочинності «складає різноманітну за формами діяльність відповідних суб'єктів (державних, недержавних органів та установ, громадських формувань та окремих громадян), які взаємодіють у вигляді системи різнорідних заходів, спрямованих на пошук шляхів, засобів та інших можливостей ефективного впливу на злочинність з метою зниження інтенсивності процесів детермінації злочинності на усіх рівнях, нейтралізації дії її причин та умов для обмеження кількості злочинних проявів до соціального толерантного рівня» [2, с. 44–45]. Організація протидії злочинності полягає у здійсненні ряду операцій (облік, реєстрація, прогнозування, планування, координація, визначення тенденцій злочинності тощо), зокрема управлінського, профілактичного характерів. Реалізація правоохоронної діяльності спеціальними суб'єктами (органами державної влади, об'єднаннями громадян і безпосередньо самими громадянами) передбачає здійснення комплексу заходів у рамках правоохоронного та правозастосовного напрямів діяльності. Попередження злочинності – це виконання уповноваженими суб'єктами запланованих і передбачених нормативно-правовими актами заходів, спрямованих на попередження розвитку та поширення злочинних намірів, визначення ознак притаманних тому чи іншому злочину, в тому числі з метою встановлення суб'єкта злочину та притягнення винної особи до відповідальності, що у свою чергу сприяє відновленню прав, свобод та інтересів осіб, які були порушені внаслідок вчинення протиправного посягання.

Із зазначеного випливає, що головним завданням забезпечення кримінологічної безпеки є досягнення умов, за яких не існує взагалі (як ідеальний варіант) або існує мінімальний рівень імовірності виникнення злочинних посягань на охоронювані спеціально уповноваженими суб'єктами права, свободи та інтереси громадян, а також інтереси держави. Виконання такого завдання вбачається можливим за допомогою здійснення діяльності пов'язаної з протидією злочинності шляхом: 1) вивчення закономірностей та особливостей поширення злочинності з метою накопичення необхідної інформації для подальшого унеможливлення зазначеного процесу; 2) недопущення формування антисоціальних настанов у осіб та девіантної поведінки, особливо у категорії потенційно схильної вчинення злочинів; 3) встановлення детермінантів злочинності та впливу на них з метою усунення; 4) попередження можливості стати реальним об'єктом протиправного посягання; 5) здійснення цілеспрямованої профілактики; 6) реалізації правоохоронної функції держави, яка забезпечується ефективною роботою правоохоронних органів.