

УДК 004.056

Владислав Сергійович Герасимюк,

курсант 4 курсу факультету № 4

Харківського національного університету внутрішніх справ

Юрій Миколайович Онищенко,

кандидат наук з державного управління, доцент,

доцент кафедри інформаційних технологій та кібербезпеки

факультету № 4 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. 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. 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).

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. Актуальною проблемою сьогодення є низький рівень комп'ютерної грамотності та кіберкультури користувачів мережі.

Проаналізувавши дані, отримані в результаті інформаційного запиту, направлено до Генеральної Прокуратури України, про статистику вчинення кіберзлочинів в Україні станом на 2018 рік, можна констатувати, що сучасний стан системи публічної безпеки не забезпечує у повному обсязі нейтралізацію існуючих кіберзагроз. Так, у 2018 році 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 Україні можна прийти до висновку, що найбільшу кількість зареєстрованих кіберзлочинів зафіксовано у наступних областях: Миколаївська – 378; Одеська – 351; Львівська – 272 та у місті Києві – 283 злочини. Найменшу кількість кіберзлочинів зареєстровано в Івано-Франківській – 20; Тернопільській – 25; Волинській – 29 та Сумській – 30 злочинів.

Аналізуючи кримінологічні характеристики осіб, що вчинили кіберзлочини у 2018 році, 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 році, 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.

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. Відповідно до отриманої статистики Генеральної Прокуратури України у 2018 кількість кримінальних проваджень, направлених до суду з обвинувальним актом зросла вдвічі і складає 1515 кримінальних справ, що свідчить про поліпшення роботи правоохоронних органів у напрямку протидії кіберзлочинам.

Способи вчинення кіберзлочинів 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 злочинів, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів є одним із важливих заходів, передбачених Стратегією кібербезпеки України.

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.

Одержано 28.10.2019