криминалистических исследований). М.: Государственное издательство юридической литературы, 1958.

3. Криминалистическое исследование документов. Образцы экспертных заключений / (сост. Павленко С. Д., Золотарь Н. С., Попов Ю. П., Мороз Т. И.). К.: РИО МВД ССР, 1989. С. 202.

4. Методика технічної експертизи документів (загальна частина) / (укл. Ковальов К. М., Давидова О. О., Коваленко В. В., Тимофеєва Т. В.). К.: ДНДЕКЦ МВС України, 2007. С. 34.

5. Методика технічної експертизи відбитків печаток та штампів (укл. Ковальов К. М., Коваленко В. В.). К.: ДНДЕКЦ МВС України, 2009. С. 19.

УДК 343. 3/. 7

Карина Олегівна ТУРЖАВСЬКА,
курсант ІІІ курсу Херсонського факультет Одеського державного університету внутрішніх справ
Роман Васильович БАРАНЕНКО,
професор кафедри професійних та спеціальних дисциплін Херсонського факультету Одеського державного університету внутрішніх справ, кандидат технічних наук, доцент

ПРИЧИНИ ВЧИНЕННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ В УКРАЇНІ

У сучасному світі встановлюється стрімке впровадження до повсякденного життя комп'ютерної техніки та комп'ютерних технологій, що надає можливість розвитку інформаційним, телекомунікаційним та інформаційно-телекомунікаційним мережам. Це ставить перед суспільством питання про необхідність захисту від протиправних посягань як особистої інформації, так і найбільш важливих сегментів національної та державної безпеки – фінансового, економічного та інформаційного. На сьогоднішній день складно собі уявити сферу діяльності, в якій не використовується комп'ютерна техніка, комп'ютерні та телекомунікаційні мережі. Жоден складний технологічний процес не може існувати без використання інноваційних технологій, соціальні мережі кожного дня залучають мільйони користувачів, кожен з яких довіряє мережі частину свого особистого життя. Однак і ця сфера «віртуальних» суспільних відносин не позбавлена вразливості.

Незаконне втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж – це проникнення до цих машин, їх систем чи мереж і вчинення дій, які змінюють режим роботи машини, її системи чи комп'ютерної мережі, або ж повністю чи частково припиняють їх роботу, без дозволу

(згоди) відповідного власника або уповноважених ним осіб, а так само вплив на роботу ЕОМ за допомогою різних технічних пристроїв, здатних зашкодити роботі машини (1).

Під несанкціонованим втручанням в роботу мереж електрозв'язку слід розуміти будь-які (окрім втручання в роботу ЕОМ, їх систем чи комп'ютерних мереж, що забезпечують роботу мереж електрозв'язку) вчинені без згоди власника відповідної мережі чи службових осіб, на яких покладено забезпечення її нормальної роботи, дії, внаслідок яких припиняється робота мережі електрозв'язку або відбуваються зміни режиму цієї роботи (1).

Причини частого вчинення злочинів у сфері комп'ютерних систем – це, насамперед, доступ кожної людини до мережі Інтернет, до комп'ютерних систем. Тобто, якщо у людини є намір вчинити злочин, то вона може знайти всю необхідну інформацію дуже швидко і у великому обсязі. Другим фактором, який грає дуже важливу роль при вчиненні комп'ютерних злочинів, є анонімність. Саме анонімність забезпечує злочинцям неможливість їх відстеження. Зазвичай особи користуються прихованими з'єднаннями, або користуються такими сайтами або програмами, які приховують їх місцезнаходження, наприклад, Tor-browser. Таким чином, злочинець набуває навичок, які використовує для вчинення наступних злочинів, а саме незаконного втручання до комп'ютерних систем. Враховуючи це, притягнення до кримінальної відповідальності за вчинення таких злочинів має певні особливості, що відображені в законах України та правових нормах.

Суспільна небезпечність комп'ютерних злочинів обумовлюється наступними факторами (2):

– впровадження різноманітних інформаційних технологій і процесів, заснованих на використанні електронно-обчислювальних машин, у багатьох сферах людської діяльності;

– високий масштабний коефіцієнт зусиль злочинців у цій сфері;

– відносна доступність для широкого кола осіб спеціальних знань і техніки, необхідної для вчинення злочину.

Для ефективної боротьби з комп'ютерними злочинами необхідно дати оцінку відповідності процесуальних норм ведення досудового розслідування і переслідування в судовому порядку вимогам часу. Рівень злочинності в кіберпросторі зростає настільки й з такою швидкістю, що законодавство просто не встигає за розвитком технологій. Комплекс заходів боротьби з комп'ютерними злочинами повинен спиратися на єдину державну політику та стратегію в цій галузі, що містить заходи державного, політичного, економічного, соціального, правового та іншого характеру.

Список бібліографічних посилань:

1. Кримінальний кодекс України. стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів),

автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. URL: http://legalexpert. in. ua/komkodeks/uk/81-uky/2070-361. html.

2. Безпека комп'ютерних систем: злочинність у сфері комп'ютерної інформації та її попередження / Вертузаєв М. С., Голубєв В. О., Котляревський О. І., Юрченко О. М. / Під заг. ред. О. П. Снігерьова. – Запорізький юридичний інститут МВС України, Національна академія внутрішніх справ України. – Запоріжжя: ПВКФ «Павел», 1998. С. 315.

УДК 343. 35

Артем Олександрович ХЛОПОВ,
аспірант Харківського національного університету внутрішніх справ
ORCID https://orcid. org/0000-0001-5342-9183

ОКРЕМІ ПИТАННЯ ВЛАСНОСТІ НА СПЕЦІАЛЬНІ ТЕХНІЧНІ ЗАСОБИ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ ТА ЇХ ОБІГУ У РАМКАХ АНАЛІЗУ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО СТ. 359 КК УКРАЇНИ

У 2010 році були внесені зміни до ст. 359 Кримінального кодексу України (далі – КК України), якими була встановлена відповідальність за придбання та збут спеціальних технічних засобів отримання негласної інформації (далі – СТЗ), при цьому законодавцем не була врахована потреба узгодити між собою окремі законодавчі акти та досягти правової визначеності. Наслідком є порушення прав і свобод громадян, вилучення побутових засобів, що можуть фіксувати інформацію про особу та притягнення громадян до кримінальної відповідальності.

Відповідно до ст. 359 КК України встановлюється відповідальність за незаконне придбання, збут або використання спеціальних технічних засобів отримання інформації (2).

Суспільна небезпечність цього злочину полягає в тому, що він порушує встановлений порядок використання спеціальних технічних засобів негласного одержання інформації, принижує авторитет органів державної влади, підриває довіру до органів, які застосовують такі засоби, посягає на конституційні права та свободи громадян (6, с. 761).

З огляду на це має бути встановлений законодавством порядок обігу СТЗ. Однак порядку обігу СТЗ чи обмеження такого обігу для приватних осіб немає. Відповідно до ст. 92 Конституції України правовий режим власності визначається виключно законом (1).

На сьогодні можна констатувати, що закону, який регулює зазначену сферу, у законодавстві нашої країни немає. Єдиним підзаконним актом, що забороняє перебування у власності громадян спеціальних технічних засобів негласного отримання інформації, є Постанова Верховної Ради України від 17. 06. 1992 № 2471-XII