УДК 343

Цимбал М.І.,
викладач кафедри історії,
соціології та правознавства
Дрогобицького державного педагогічного
університету ім. І. Франка

ІНОЗЕМНИЙ ДОСВІД КРИМІНАЛЬНО-ПРАВОВОЇ ПРОТИДІЇ НЕЗАКОННОГО ПОВОДЖЕННЯ ІЗ СПЕЦІАЛЬНИМИ ТЕХНІЧНИМИ ЗАСОБАМИ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Анотація. У статті проаналізовано особливості використання спеціальних технічних засобів виходячи з кримінально-правових позицій. Досліджено досвід зарубіжного кримінально-правового забезпечення незаконного використання спеціальних засобів у порівнянні зі ст. 359 КК України.

Аннотация. В статье проанализированы особенности использования специальных технических средств исходя из уголовно-правовых позиций. Исследован опыт зарубежного уголовно-правового обеспечения незаконного использования специальных средств, в сравнении со ст. 359 УК Украины.

Annotation. . The aspects of using the special technical tools are analyzed in article from the criminal legal point of view. The experience of the foreign criminal legal providing of the illegal use of such tools is looked at, comparing with the 359th article of the Criminal Code of Ukraine

Постановка проблеми. Суспільні відносини під час науково-технічного прогресу потребують на постійне вдосконалення нормативного регулювання. Використання новітніх технологій у різних сферах іноді створює нові загрози для окремих соціальних цінностей. Виникнення нового виду технічних засобів– спеціальних технічних засобів негласного отримання інформації (далі – СТЗНОІ) та бурхливе зростання їх кількості, вдосконалення якості та постійне розширення сфер потенціального використання потребують на встановлення цілісної системи норм правового забезпечення вказаних процесів, зокрема їх кримінально-правового аспекту. Виникнення якісно нових суспільних відносин, що пов'язані з використанням СТЗНОІ, супроводжується появою та розповсюдженням нового виду посягань, які порушують ці відносини. Це обумовило наявність у чинному Кримінальному кодексі (далі – КК) ст. 359, що встановлює кримінальну відповідальність за незаконне поводження із СТЗНОІ [2].

Попри той факт, що перші згадки про кримінальну відповідальність за злочини у сфері незаконного використання СТЗНОІ з'явилися у вітчизняній кримінально-правовій доктрині, а потім й у кримінальному законодавстві ще до ухвалення КК 2001 р., в Україні досі існує значна кількість проблем, пов'язаних з кримінальними посяганнями, в яких використовуються СТЗНОІ. Ці проблеми мають великий ступінь дискусійності та потребують на ефективне й оперативне вирішення. Крім

іншого, потребує на встановлення характер і ступінь суспільної небезпеки злочинів, пов'язаних з незаконним використанням СТЗНОІ, об'єктивні і суб'єктивні ознаки злочину, передбаченого ст. 359. Існує нагальна потреба в узгодженні та вдосконаленні термінологічного апарата, який має використовуватися при формулюванні кримінально-правових та інших норм, що регулюють процеси виготовлення, обігу й використання СТЗНОІ; велику проблему становлять питання щодо характеру та змісту предмета та об'єкта такого злочину, як незаконне поводження із СТЗНОІ; у кримінально-правовій доктрині досі не проаналізовано зарубіжний досвід протидії посяганням на інформацію з використанням спеціальних засобів, відсутні й пропозиції щодо вдосконалення кримінально-правового законодавства у цій сфері, залишаються невирішеними проблеми криміналізації і декриміналізації поводження із СТЗНОІ.

Ступінь наукової розробки теми. Певні аспекти відповідальності за незаконне поводження із СТЗНОІ містяться у роботах П.П. Андрушка, В.П. Анчукова, П.С. Берзіна, В.М.Бутузова, В.Б. Вехова, Ю.М. Громова, В.О. Копилова, М.О.Корчевського, В.Д. Курушина, А.М. Ришелюка, Д.О. Янишевського тощо. Однак в Україні до цього часу відсутні окремі, самостійні наукові роботи, присвячені дослідженню вказаного злочину.

Необхідність у глибокому комплексному дослідженні проблем кримінальної відповідальності за незаконне використання СТЗНОІ, є викликаною, зокрема, й великою кількістю практичних питань, що виникають при кваліфікації незаконного використання різних технічних засобів й приладів у інформаційній сфері потребує у дослідженні іноземного досвіду, що є метою нашої статті. При цьому її завданнями слід вважати визначення із особливостями кримінально-правової кваліфікації відповідних діянь за законодавством різних розвинутих держав; проведення відповідних компаративістських досліджень. Вважаємо, що об'єктивний аналіз норм статті 359 КК України є неможливим без урахування досвіду окремих країн у встановленні кримінальної відповідальності за суспільно небезпечні дії, пов'язані з СТЗНОІ. Такий досвід має допомогти не лише критично сприймати відповідні положення вітчизняного КК, але й дозволить висунути певні пропозиції й зауваження стосовно можливих змін у кримінальному законодавстві України.

Тому *метою статті* є вивчення іноземного досвіду кримінально-правової протидії незаконного поводження із спеціальними технічними засобами негласного отримання інформації.

Викладення основного матеріалу. Кримінальне законодавство багатьох держав не встановлює відповідальність за незаконне використання спеціальних технічних засобів у вигляді окремої норми. Але у такому випадку використання спеціальних технічних засобів розглядається, як кваліфікуюча або навіть обов'язкова ознака окремих злочинів.

Так, КК Російської Федерації 1996 р. у ч. 2 ст. 138 розглядає використання спеціальних технічних засобів, призначених для негласного

отримання інформації, як обтяжуючу ознаку такого злочину, як порушення таємниці листування, телефонних переговорів, поштових, телеграфних чи інших повідомлень [11]. У ч. 2 ст. 143 КК Республіки Казахстан від 16 липня 1997 року містяться абсолютно аналогічні положення. У КК Республіки Казахстан, крім того, використання спеціальних технічних засобів є однією з можливих ознак об'єктивної сторони такого злочину, передбаченого ч. 1 ст. 200, як збирання відомостей, що складають комерційну чи банківську таємницю [9].

У ч. 2 ст. 179 КК Білорусі використання спеціальних технічних засобів, призначених для негласного отримання інформації є обтяжуючою ознакою такого злочину, як незаконне збирання або поширення відомостей про приватне життя, які складають особисту або сімейну таємницю іншої особи, без його згоди, що заподіяло шкоду правам, свободам та законним інтересам потерпілого; у ч. 2 ст. 203 використання таких засобів є обтяжуючою ознакою такого злочину, як навмисне незаконне порушення таємниці листування, телефонних або інших переговорів, поштових, телеграфних або інших повідомлень громадян [7]. Зауважимо, що у наведених нормах КК Білорусі, Росії та Казахстану обтяжуючою ознакою рівної значущості є вчинення відповідних злочинів посадовою особою з використанням службового становища.

Слід вказати, що КК Російської Федерації та КК Республіки Казахстан у ч. 3 наведених відповідно ст. 138 та ст. 143 («Порушення таємниці листування, телефонних переговорів, поштових, телеграфних чи інших повідомлень») окремою нормою встановлюють кримінальну відповідальність за «незаконні виробництво, збут або придбання з метою збуту спеціальних технічних засобів, призначених для негласного отримання інформації», тобто саме за обіг спеціальних технічних засобів [11], [9]. При цьому за розмірами покарання такий злочин слід вважати більш суспільно небезпечним, чим наведені вище злочини передбачені ч. 2 с. 138 та ч. 2 ст. 143 відповідно. Доцільність криміналізації обігу СТЗНОІ є досить дискусійним питанням; але зауважимо, що за будь-яких обставин об'єкт такого суспільно небезпечного діяння не є тотожним та навіть близьким до об'єкта незаконного отримання інформації, тому розміщення вказаних норм в рамках загальної статті КК не слід вважати доцільним.

У КК інших країн така нетотожність об'єктів ураховується: так, наведений КК Білорусі встановлює кримінальну відповідальність за незаконні виготовлення або придбання з метою збуту або збут спеціальних технічних засобів, призначених для негласного одержання інформації у окремої ст. 376, при чому ця стаття міститься у Главі 33 Особливої частини КК «Злочини проти порядку управління». При цьому у ч. 2 цієї статті встановлюються такі кваліфікуючі ознаки цього злочину, як повторність, вчинення злочину групою осіб за попередньою змовою, або посадовою особою з використанням своїх службових повноважень, а у ч. 3 цієї ж статті – вчинення цього злочину організованою групою [7].

Кримінальний кодекс Китайської Народної Республіки не передбачає використання СТЗНОІ, як обтяжуючу ознаку певних злочинів, але встановлює кримінальну відповідальність як за незаконне виробництво і продаж приладів схованого прослуховування, схованого спостереження та іншої спеціальної розвідувальної апаратури (ст. 283), так й за незаконне використання спеціальної апаратури для схованого прослуховування, схованого спостереження, яке призвело до серйозних наслідків (ст. 284). Цікаво, що злочин, передбачений ст. 283 КК Китаю, тягне покарання у вигляді позбавлення волі на термін до 3 років, а вчинення злочину, передбачений ст. 284 КК, карається позбавленням волі на термін до 2 років, тобто незаконне використання СТЗНОІ у Китаї вважається менш суспільно небезпечним, чим їх виготовлення, навіть при тому, що злочин, передбачений ст. 284 КК Китаю, має матеріальний склад, а у ст. 283 склад злочину є формальним [5, с. 190].

Кримінальний кодекс Естонії не містить в собі спеціальної норми, яка б встановлювала відповідальність за незаконне використання СТЗНОІ, але ст. 133-1 КК Естонії криміналізує незаконну оперативно-розшукову діяльність, при чому використання СТЗНОІ, як «виключні оперативно-розшукові дії» фактично є кваліфікованим злочином, передбаченим у ч. 2 ст. 133-1 КК Естонії. У ст. 133-2 КК Естонії встановлюється кримінальна відповідальність за обіг СТЗНОІ, а саме – за «виготовлення, придбання, зберігання, перевезення, продаж або передачу допоміжних засобів, які дозволяють здійснити негласне збирання та запис інформації з метою проведення незаконних виключних оперативно-розшукових дій» [14, с. 128-129].

КК Франції у ст. 226-3 встановлює кримінальну відповідальність за виготовлення, ввіз, збереження, виставляння для продажу, пропозицію, прокат або продаж, при відсутності офіційного дозволу, приладів, призначених для виявлення та фіксації розмов на відстані, для перехоплення, розкрадання, використання чи розголошення повідомлень, відправлених, переданих чи отриманих за допомогою засобів телекомунікації. Цікаво, що однакове до встановленого у ст. 226-3 покарання встановлюється у ч. 3 цієї ж статті й за рекламування вказаних приладів, якщо ця реклама підбурює до здійснення такого злочинного діяння. Зауважимо, що ч. 2 ст. 226-15 КК Франції встановлює однакову відповідальність як за перехоплення, розкрадання, чи використання розголошення повідомлень, відправлених, переданих чи отриманих за допомогою засобів телекомунікації, так й за установку технічних пристроїв, призначених для здійснення таких перехоплень [12, с. 347, 253]. Фактично, КК Франції, встановивши досить широкі критерії криміналізації обігу СТЗНОІ, не вважає використання СТЗНОІ обтяжуючою ознакою злочинів. Що посягають на конфіденційність відомостей, та передбачає кримінальну відповідальність за використання СТЗНОІ в окремих випадках.

Кримінальний кодекс Швеції встановлює кримінальну відповідальність у ст. 9a та 9b Розділу 4 «Про злочини проти волі та суспільного спокою» відповідно за прослухування бесіди, розмови або звукового відтворення та за порушення телекомунікаційної таємниці, при чому використання технічних засобів є необхідною ознакою цих злочинів. Таку кримінально-правову конструкцію слід вважати перехідною від розглядання, використання СТЗНОІ як обтяжуючої ознаки певних злочинів до криміналізації незаконного використання СТЗНОІ, як окремого злочину [13, с. 46-47].

У багатьох кримінальних законах використання СТЗНОІ розглядається як одна з можливих, або не обов'язкова (тобто, альтернативна) кваліфікуюча ознака складу певних злочинів. Так, у п. 3 ч. 1 параграфу 263 КК Данії використання обладнання для прослуховування та запису аудіоінформації вказується як одна з можливих ознак злочину, передбаченого ч. 1 цього параграфу. При цьому обтяжуючою обставиною такого злочину є посягання на торгові секрети фірми, тобто, на комерційну таємницю. Особливістю складу наведеного злочину є те, що особи, які не приймали участь у використанні вказаних СТЗНОІ, але отримали або незаконно використали інформацію, яка була розголошена внаслідок вчинення такого злочину, також притягуються до кримінальної відповідальності по ч. 1 параграфу 263 КК Данії [3, с. 192].

У КК Іспанії використання технічних засобів прослухування, передачі, запису або відтворення звуку, зображення або іншого сигналу комунікації є альтернативною ознакою злочину, передбаченого ст. 536. Цікаво, що цей злочин може бути вчинений лише спеціальним суб'єктом (посадовою особою, державним службовцем або представником влади). В ч. 1 ст. 170 КК Болгарії використання спеціальних технічних засобів є однією з альтернативних ознак об'єктивної сторони такого злочину (разом з насиллям, погрозою, хитрістю, зловживанням службовим становищем), як порушення недоторканості чужого житла, приміщення або транспортного засобу, а в ч. 3 ст. 171 КК цієї ж країни використання таких засобів є вже обтяжуючою ознакою складу іншого злочину – порушення недоторканості кореспонденції [8, с. 165, 127-128]. Зауважимо, що злочин, передбачений ч. 1 ст. 170 КК Болгарії, є злочином приватного звинувачення.

Кримінальний кодекс Литовської Республіки від 26 вересня 2000 р. у ст. 295 встановлює кримінальну відповідальність за незаконну установку або використання спеціальної техніки для збору інформації [6, с. 115]. Таким чином, об'єктивна сторона такого злочину дає можливість вважати його закінченим на більш ранньої стадії діяння, чим, наприклад, об'єктивна сторона ч. 359 КК України. Але вважаємо недоцільним встановлення кримінальної відповідальності за установку СТЗНОІ у вітчизняному кримінальному законодавстві. В умовах, коли СТЗНОІ незаконно встановлено, але його ще не почали використовувати, варто говорити про замах на злочин, а не про його вчинення.

Додамо, що кримінальні закони окремих країн (наприклад, Республіки Польща) взагалі не містять згадки про використання або обіг спеціальних технічних засобів. У цих актах кримінальна відповідальність встановлюється лише за незаконне отримання певних видів інформації та відомостей взагалі, без згадки про засоби такого отримання [10].

Як ми побачили, криміналізація незаконного використання СТЗНОІ у багатьох країнах відбувається двома основними шляхами – встановленням кримінальної відповідальності безпосередньо за використання СТЗНОІ (у вигляді окремої норми кримінального закону, або через визнання незаконного використання СТЗНОІ необхідною або альтернативною ознакою об'єктивної сторони певних злочинів), або розглядання такого використання як обтяжуючої ознаки певних злочинів. При цьому не виявлено випадків, аналогічних ситуації в КК України, коли використання СТЗНОІ є водночас самостійним складом злочину та обтяжуючою ознакою іншого злочину. У багатьох іноземних КК є кримінализованим й незаконний обіг СТЗНОІ, при чому за розміром покарання цей злочин, як правило, вважається більш тяжким, чим незаконне використання СТЗНОІ. Встановлення кваліфікованого складу незаконного використання СТЗНОІ не характерно для кримінального законодавства більшості держав.

Зауважимо, що санкції за незаконне використання СТЗНОІ (або за інші злочини, формою вчинення яких може бути незаконне використання СТЗНОІ) у різних кримінально-правових законах мають досить нерівний розмір, але загальним правилом є призначення покарання у вигляді позбавлення волі на різні строки (Іспанія – від 2 до 6 років, Естонія – до 5 років, Литва, Данія – до 4 років, Білорусь – до 3 років, Болгарія, Китай – до 2 років, Франція – до 1 року). Таким чином, найвищий розмір покарання, встановлений санкцією у ч. 1 ст. 359 КК України (позбавлення волі строком до чотирьох років) слід визнати таким, що відповідає іноземним аналогам. Зауважимо, що в жодному кримінальному законі нами не було знайдено згадки про конфіскацію спеціальних технічних засобів, як вид покарання. Це робить досить непереконливою позицію Ахтирської Н., яка критикує законодавче вирішення проблеми визначення відповідальності за дії, передбачені ст. 359 КК України, через те, що у санкції цієї статті відсутня конфіскація, в той час, коли за злочини у сфері інформаційних систем, в частинах 1 та 2 ст. 361 КК України передбачена конфіскація програмних та технічних засобів, призначених для проникнення у електронно-обчислювальні машини [1].

Висновки. Висловимо думку про те, що конфіскація СТЗНОІ не вважається доцільною насамперед через те, що правом власності на такі технічні засоби здебільшого користується обмежене коло осіб, тому злочинець, як правило, використовує СТЗНОІ, яке йому не належить (наприклад, службовій особі правоохоронних органів не належать СТЗНОІ, якими вона користується). До того ж навіть при наявності у злочинця певних прав на технічній засіб, він може бути позбавлений цих прав як у

кримінально-процесуальному порядку (в силу того, що СТЗНОІ виступає засобом вчинення злочину), так і адміністративно (через ануляцію дозволу на володіння або власність на СТЗНОІ тощо). Тому вважаємо за непотрібне пропонувати зміни характеру покарань, які передбачені у ч. 1 ст. 359 КК України. У той же час слід визнати що гармонізація кримінального законодавства України відповідно до стандартів Європейського Союзу у майбутньому потребує на додаткові наукові роботи у сфері європейського досвіду боротьби з незаконним використанням СТЗНОІ.

Використані джерела:

1. Ахтырская Н. О совершенствовании уголовного законодательства Украины в сфере борьбы с киберпреступностью [Електронний ресурс] – Режим доступу до сайту : http://www.crime-research.ru/library/Akhtirsk0403.html
2. Кримінальний кодекс України від 5 квітня 2001 р., із змінами та доповненнями, станом на 1 листопада 2010 р. // Офіційний сайт Верховної ради України [Електронний ресурс]. – Режим доступу до сайту : http://www.portal.rada.gov.ua/
3. Уголовный кодекс Дании [науч. ред. С. С. Беляева] / Законодательство зарубежных стран. Ассоциация Юридический центр. – СПб : Юридический центр Пресс, 2001. – 243 с.
4. Уголовный кодекс Испании [под ред. Н. Ф. Кузнецова, Ф. Ш. Решетникова]. – М. : Зерцало, 1998. – 205 с.
5. Уголовный кодекс Китайской Народной Республики [под ред. А. И. Коробеева, пер. с кит. Д. В.Вичикова]. – СПб. : Юридический центр Пресс, 2001. – 303 с.
6. Уголовный кодекс Литовской Республики : утвержден законом № VIII-1968 26 сентября 2000 г. [науч. ред. В. Павилониса] / Законодательство зарубежных стран. Ассоциация Юридический центр. – СПб : Юридический центр Пресс, 2002. – 167 с.
7. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З // Офіційний сайт Верховної ради України [Електронний ресурс]. – Режим доступу до сайту : http://www.portal.rada.gov.ua/
8. Уголовный кодекс Республики Болгария [науч. ред. А. И. Лукашова] / Законодательство зарубежных стран. Ассоциация Юридический центр. – СПб : Юридический центр Пресс, 2001. – 182 с.
9. Уголовный кодекс Республики Казахстан от 16 июля 1997 года № 167-1 // Офіційний сайт Верховної ради України [Електронний ресурс]. – Режим доступу до сайту : http://www.portal.rada.gov.ua/
10. Уголовный кодекс Республики Польша с изм. и доп. на 1 августа 2001 г. [науч. ред. А. И. Лукашова, Н. Ф. Кузнєцова] / Законодательство зарубежных стран. Ассоциация Юридический центр. – СПб : Юридический центр Пресс, 2001. – 189 с.
11. Уголовный кодекс Российской Федерации от 24 мая 1996 г. // Юридический вестник. – 1996. – № 13. – С. 3–68.
12. Уголовный кодекс Франции [науч. ред. Л. В. Головко, И. Е. Крыловой ; пер. и пред. Н. Е. Крыловой. – СПб. : Юридический центр Пресс, 2002. – 650 с.
13. Уголовный кодекс Швеции [науч. ред. Н. Ф. Кузнецова и С. С. Беляев ; пер. С. С. Беляева]. – СПб. : Юридический центр Пресс, 2001. – 320 с.
14. Уголовный кодекс Эстонской Республики с изм. и доп. на 1 августа 2001 г. [науч. ред. В. В. Запевалова] / Законодательство зарубежных стран. Ассоциация Юридический центр. – СПб : Юридический центр Пресс, 2001. – 193 с.

Рецензент: к.ю.н., професор Литвин О.П.