4. Тропина Т.Л. Киберпреступность : понятие, состояние, уголовно-правовые меры борьбы [Електронний ресурс] / Т. Л. Тропинина // Сайт Владивостокського центру дослідження організованої злочинності. – Режим доступу : http://www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb =1&pb=1.

5. Грицун О.О. Кримінальний аспект міжнародної інформаційної безпеки / О. О. Грицун // Право і суспільство. – 2015. – № 6. – Ч. 2. – с. 142-147.

6. Конвенція про кіберзлочинність // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.

Питання термінології у визначенні системи злочинів в сфері ІТ (досвід інших держав)

Дмитрук М.М.
кандидат юридичних наук, доцент
доцент кафедри кримінального права
Національного університету «Одеська юридична академія»

5 жовтня 2017 р. Президентом України підписано Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [1]. Прийняття вказаного закону покращує правове регулювання протидії кіберзлочинності, визначає окремі поняття, які мають безпосереднє відношення і до законодавства про кримінальну відповідальність, проте взаємозв'язок та взаємовплив вказаного акту із КК України залишився достатньо примарним.

У п. 8, ст. 1 вказаного законодавчого акту надано визначення «кіберзлочину» (комп'ютерного злочину), яким визначається, суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. Поряд із цим, сам КК України не містить згадки про поняття кіберзлочину або комп'ютерного злочину, а сама система злочинів у Розділі XVI О. ч. КК України іменується як «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Питання термінології злочинів, які посягають на суспільні відносини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку досліджувалось вченими неоднократно, проте узагальнена позиція з цього питання не сформована.

Так, М.В. Карчевський зазначає: «Поняття «комп'ютерний злочин» та «кіберзлочин», в загальновизнаному розумінні можуть бути ефективно використані при проведення кримінологічних, кримінально-процесуальних, криміналістичних досліджень. Що ж стосується національного кримінально-правового дискурсу, то тут застосування цього поняття слід обмежити, і використовувати запропоноване поняття «злочини в сфері використання інформаційних технологій» [2, с. 14]. При цьому вчений у якості доводів аналізує поняття «злочини у сфері ІТ», «інформаціна безпека» та приходить до висноку: «Таким чином, злочини в сфері використання інформаційних технологій, є одним з видів злочинів в сфері інформаційної безпеки, є передбачені КК України, суспільно небезпечні, винні, вчинені суб'єктом злочину діяння, які заподіюють шкоду, забезпеченим засобами обчислювальної техніки, відносинам у сфері реалізації інформаційної потреби. Аналіз чинного КК дозволяє прийти до висновку, що до таких злочинів слід відносити посягання, передбачені ст. ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 КК [2, с. 11]. Вказане твердження М.В. Карчевського щодо віднесення до «злочинів в сфері використання ІТ» належать виключно вказані діяння залишається необгрунтованим. Якщо погодитись із вказаним вченим, то виходить, що порушення авторських та суміжних прав, яке здійнюється шляхом втручання в роботу ЕОМ не заподіює шкоду «відносинам у сфері реалізації інформаційної потреби» і не вчиняється за допомогою саме «засобів обчислювальної техніки». Проте ситуація є зовсім протилежною. Інші доводи із боку вказаного вченого наведено на користь позначення злочинів передбачених у Розділі XVI О. ч. КК України як «злочинів в сфері використання ІТ» не наведено.

Для етимологічного розуміння, що таке «інформаціна технологія» і чи можна систему злочинів передбачених в Розділі XVI О. ч. КК України визначити як «злочини в сфері інформаціних технологій» розглянемо що таке «інформаційні технології».

«Інформаційна технологія», згідно ст. 1 ЗУ «Про Національну програму інформатизації», – це цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування

[3]. Таке ж визначення цього поняття міститься у «Методиці визначення належності бюджетних програм до сфери інформатизації» затвердженої Наказом Держкомзв'язку від 06.06.2003 № 97 [4]. Вказане визначення є досить широким і не дає можливості встановити тотожність між поняттям «сфера інформаційних технологій» та «сукупність суспільних відносин, що охороняються положеннями Розділу XVI О. ч. КК України».

В Конвенції про кіберзлочинність від 23.11.2001 р. (ратиф. ЗУ № 2824-IV від 07.09.2005 р.) до кіберзлочинів віднесено: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6)); 2) правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8)); 3) правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією (ст. 9)); 4) правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10). В Преамбулі Конвенції з кіберзлочинності також згадується, що її положення спрямовані на «бортьбу із кіберзлочинністю» та «захист законних інтересів у ході використання і розвитку інформаційних технологій». Тобто за змістом системі злочинів згідно Конвенції про кіберзлочинність відповідає визначення «кіберзлочину», яке передбачено положеннями п. 8) ст. 1 ЗУ «Про основні засади забезпечення кібербезпеки України», а захист «інформаціних технологій» виступає як одне із завдань Конвенції про кіберзлочинність.

У зв'язку із цим, цікавим є питання як визначається досліджувана система злочинів в кримінальному законодавстві інших держав, до яких КК України є близьким за структурою.

В КК Грузії Глава XXXV визначає вказану систему злочинів, як «Кіберзлочини», таку ж назва має Глава 30 в КК Азербайджану.

В КК Вірменії вказана система злочинів, згідно Глави 24, іменується як «Злочини проти безпеки комп'ютерної інформації», в КК Білорусії, згідно із Розділом XII, – «Злочини проти інформаційної безпеки», яка містить одну Главу 31 «Злочини проти інформаційної безпеки». В КК Киргизької Республіки Глава 42 також визначає систему злочинів як «Злочини проти інформаційної безпеки», такою ж є назва Розділу XII в КК Республіки Таджикистан.

В КК Туркменістану досліджувана система злочинів, згідно Розділу XIII, визначається як «Злочини в сфері комп'ютерної інформації», який містить одну Главу 33 під назвою «Злочини в сфері інформатики і зв'язку». В КК Естонії подібним чином, згідно Глави 14, визначається досліджувана система злочинів як «Злочини в сфері комп'ютерної інформації та обробки даних». Дещо іншу назву має Глава 7 КК Казахстану «Кримінальні правопорушення в сфері інформатизації та зв'язку». В КК РФ згідно Глави 28 вказана система злочинів іменується як «Злочини в сфері комп'ютерної інформації». В КК Литовської Республіки досліджувана система злочинів, згідно Глави XXX, іменується як «Злочини проти інформатики». І лише в КК Республіки Узбекистану досліджувана система злочинів, згідно Глави XX-1, визначається як «Злочини в сфері інформаційних технологій».

Отже, дослідження назви системи злочинів більшості державн СНД та інших пострадянських держав свідчить, що вказана система злочинів визначається, як: 1) кіберзлочини; 2) злочини проти інформаційної безпеки; 3) злочини проти комп'ютерної інформації (або інформатики) та зв'язку; 4) злочини в сфері інформаційних технологій. Тобто у більшості пострадянських держав законодавець ніде не перелічує предмети або засоби вчинення злочину для позначення назви злочинів в сфері ІТ. Такий спосіб визначення системи злочину (або назви родового об'єкту (не стосується Розділу XIX О. ч. КК України)), як перелічення у назві конкретихованих предметів суспільних відносин, законодавцем використано в Розділі XX, XIV, XIII. Вказаний спосіб наврядчи можна визнати вдалим.

Враховуючи, що поняття кіберзлочину або комп'ютерного злочину, згідно нового ЗУ «Про основні засади забезпечення кібербезпеки України», використовується стосовно як злочинів, які посягають на суспільні відносини, що охороняються положеннями Розділу XVI О. ч. КК України, так і злочинів, які посягають на будь-які інші суспільні відносини шляхом застосування інформаційних технологій, оптимальним було визначити діяння, відповідальність за які передбачено у ст. ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України як «злочини в сфері інформаційних технологій», як це передбачено у КК Узбекистану. Поряд із цим, вказаний поділ на кіберзлочини (комп'ютерні злочини) та злочини в сфері ІТ є досить умовним, оскільки за змістом законодавче поняття «інформаціні технології» охоплюють більше коло суспільних відносин, ніж ті, які охороняються положеннями Розділу XVI О. ч. КК України, а поняття «кіберзлочин» та «інформаційні технології» використовуються в Конвеції про кіберзлочинність як різнопорядкові поняття.

Література:

1. Про основні засади забезпечення кібербезпеки України: ЗУ від 05.10.2017 р. № 2163-VIII. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/2163-19

2. Карчевский Н.В. Киберпреступление или преступление в сфере использование информационных технологий? // Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. – Одеса : ОДУВС, 2016. – С. 10-15.

3. Про Національну програму інформатизації: ЗУ від 04.02.1998 р. № 74/98-ВР. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/74/98-вр

4. Методики визначення належності бюджетних програм до сфери інформатизації: Наказ Держкомзв'язку та інформацтизації України від 06.06.2003 р. № 97. – Режим дост.: http://zakon3.rada.gov.ua/laws/show/z0512-03.

Правові засади регулювання забезпечення кібербезпеки в Україні

Ігнатушко Ю.І.
кандидат юридичних наук
доцент кафедри інформаційних технологій та
кібернетичної безпеки Національної академії внутрішніх справ

Однією зі сфер правового регулювання , що зазнають впливу інтеграційних процесів і уніфікації, є вироблення єдиного комплексного підходу , розробка правових та організаційних засад регулювання кібербезпеки в Україні , розв'язання проблем використання неліцензійного комп'ютерного програмного забезпечення.

До останнього часу безпека інформації в автоматизованих системах (АС) розумілася виключно як небезпека її несанкціонованого отримання протягом усього часу обробки і зберігання в АС.

Сьогодні безпека інтерпретується ще й як безпека дій, для виконання яких використовується інформація.

Принципові відмінності розширеного тлумачення, на відміну від традиційного, дуже важливі, оскільки обчислювальна техніка все більше використовується для автоматизованого управління інформаційними системами і процесами, в яких несанкціоновані зміни запланованих алгоритмів і технологій можуть мати серйозні наслідки.

Історично традиційним об'єктом права власності є матеріальний об'єкт.

Інформація, як об'єкт права власності, легко переміщується до іншого суб'єкта права власності без помітного порушення права власності на інформацію. Переміщення матеріального об'єкта до іншого суб'єкта права власності неминуче і, як правило, спричиняє втрату цього об'єкта первинним суб'єктом права власності, тобто, відбувається очевидне порушення його права власності.

Небезпека копіювання і переміщення інформації посилюється тим, що вона, як правило, відчужувана від власника, зберігається і обробляється в сфері доступності значної кількості суб'єктів, які не є суб'єктами права власності.

Розглянувши особливості інформації, як об'єкта права власності, зазначимо, що в іншому інформація, очевидно, нічим не відрізняється від традиційних об'єктів права власності.

Право власності включає три складових елементи права власності: право розпорядження; право володіння; право користування. Суб'єкт права власності на інформацію може передати частину своїх прав (розпорядження), не втрачаючи їх сам, іншим суб'єктам, наприклад - власникові матеріального носія інформації (це - володіння або користування) або користувачеві (це - користування, володіння).

Для інформації право розпорядження має на увазі виняткове право (ніхто інший, крім власника) визначати, кому ця інформація може бути надана у володіння чи користування [1, с. 27].

Право володіння передбачає мати інформацію в незмінному вигляді. Право користування має на увазі право використання цієї інформації у власних інтересах. Таким чином, до інформації, крім суб'єкта права власності на інформацію, можуть мати доступ інші суб'єкти права власності як законні, санкціоновані (це - суб'єкти права на елементи власності), так і незаконні, несанкціоновані. Виникає складна система взаємовідносин між цими суб'єктами права власності. Ці взаємовідносини повинні регулюватися й охоронятися, оскільки відхилення від них можуть призвести до переміщення інформації, що спричиняє порушення права власності суб'єкта на інформацію.

На державному рівні для гарантування кібернетичної безпеки вживаються наступні заходи: здійснюється формування і реалізація єдиної державної політики щодо забезпечення захисту