

Література:

1. Чи є віртуальна власність власністю? [Електронний ресурс] // Дитячий майданчик. – 2011. – Режим доступу до ресурсу: http://www.playground.ru/blogs/other/yavlyaetsya_li_virtualnaya_sobstvennost_sobstvennostyu-39202/.
2. Цивільний кодекс України: чинне законодавство із змінами та допов. на 01 вересня 2017 року: Офіц. Текст. – К.: Алерта, 2017 – 306 с.
3. Рузавин Г. И. Виртуальность // Новая философская энциклопедия / Ин-т философии РАН; Нац. обществ.-науч. фонд; Предс. научно-ред. совета В. С. Стёпин, заместители предс.: А. А. Гусейнов, Г. Ю. Семигин, уч. секр. А. П. Огурцов. — 2-е изд., испр. и допол. — М.: Мысль, 2010. — 324 с.
4. 2005 Ferrari FXX [Електронний ресурс] // supercars.net. – 2011. – Режим доступу до ресурсу: <https://www.supercars.net/blog/2005-ferrari-fxx/>.
5. Пилипенко Г. М. Економічні пріоритети України як основа формування національної моделі випереджального розвитку : дис. докт. ек. наук : Д 08.080.0 / Пилипенко Ганна Миколаївна – Дніпропетровськ, 2009. – 102 с.
6. Обезумевший геймер [Електронний ресурс] // Жёлтая пресса. – 2010. – Режим доступу до ресурсу: <http://yellowpress.ws/?public=3071>.
7. Public Act No. 05-136 [Електронний ресурс] // Connecticut state. – 2005. – Режим доступу до ресурсу: <https://www.cga.ct.gov/2005/act/Pa/2005PA-00136-R00SB-00262-PA.htm>.
8. Senate Bill SB 301 [Електронний ресурс] // state Georgia. – 2015. – Режим доступу до ресурсу: <http://www.legis.ga.gov/legislation/en-US/Display/20172018/SB/301>.
9. Fiduciary Access to Digital Assets Act, Revised [Електронний ресурс] // The National Conference of Commissioners on uniform state laws. – 2015. – Режим доступу до ресурсу: [http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20\(2015\)](http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015))

Правова охорона конфіденційності та персональних даних в мережі Інтернет

Маковій В.П.

кандидат юридичних наук, доцент
завідувач кафедри цивільно-правових дисциплін ОДУВС

Кіберзлочинність як соціально-правове поняття відтворене в багатьох джерелах, зокрема воно ототожнюється з сукупністю інформаційних злочинів поєднаних певними характерними рисами, серед яких навмисність протиправних дій, спрямованих як правило на розкрадання або руйнування інформації, єдність об'єкту – суспільні відносини в сфері обігу інформації різного походження в інформаційних системах і мережах, наявність корисливого чи хуліганського мотиву [1].

Відповідно до положень Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року під останньою необхідно розуміти сукупність злочинів, поєднаних в наступні групи: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, правопорушення безпосередньо пов'язані з використанням комп'ютера як засобу скоєння злочину, правопорушення, пов'язані зі змістом даних (інформації), розміщеної в комп'ютерних системах, правопорушення, пов'язані з порушенням авторських та суміжних прав, а також акти расизму та ксенофобії, вчинені за допомогою комп'ютерних систем.

В наведеному відображені правопорушення щодо конфіденційної інформації та персональних даних в комп'ютерних системах, що вимагає встановити сутність правової охорони таких об'єктів суспільних відносин з використанням комп'ютерних мереж, зокрема Інтернет.

В чинному законодавстві сутність конфіденційної інформації переплітається з поняттям персональних даних, де останнє як правило розглядається як підмножина першого.

У відповідності до ст. 1 Закону України “Про інформацію” інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, а захист інформації - це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

За правовим режимом виділяють різні види інформації. Згідно ст. 3 Конституції України людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Стаття 32 Основного Закону України забороняє збирання, зберігання, використання

та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Наведені положення закладають основи до правового відшукування компромісу між правом на захист приватних даних і правом на свободу інформації (вільний доступ до інформації), де перше відображає приватний інтерес, а друге публічний [2, с. 223].

Частина 1 ст. 7 Закону України «Про доступ до публічної інформації» визначає конфіденційну інформацію — як інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 вказаного Закону. У відповідності до ч. 2 ст. 7 цього Закону розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди — лише в інтересах національної безпеки, економічного добробуту та прав людини.

Рішенням Конституційного суду України від 30 жовтня 1997 року № 5-зп до конфіденційної інформації віднесено також відомості про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані) [3], а рішенням цієї ж судової інстанції від 20 січня 2012 року №2-рп/2012 такою інформацією є відомості про особисте та сімейне життя особи, тобто будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень [4].

Наведені положення створили передумови для прийняття спеціального законодавства в сфері захисту інформації про людину, яку згідно ст. 21 Закону України «Про інформацію» прийнято відносити до інформації з обмеженим доступом. Основою подібного законодавства є Закон України «Про захист персональних даних», згідно ст. 6 якого обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством. Така позиція віднайшла відповідне обґрунтування й у правовій науці [5, с. 8]

Порядок доступу до персональних даних третіх осіб визначений ст. 16 Закону України «Про захист персональних даних», де вказано перелік інформативних даних, що зазначаються у запиті, а також які повідомляються суб'єктам персональних даних згідно ст. 21 цього Закону. Наведена стаття встановлює правовий механізм обмеження права на конфіденційну інформацію, що вміщує персональні дані про особу.

Кваліфікованим обмеженням права на конфіденційність інформації про особу є віднесення її до публічної інформації у контексті положень ст. 10¹ Закону України «Про захист персональних даних», тобто такої, що була відображена та задокументована будь-якими засобами та на будь-яких носіях, була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом. Критеріями обмеження її правового режиму виступають: знеособленість та захищеність персональних даних про особу відповідного до даного Закону, наявність згоди осіб, чиї персональні дані містяться в інформації у формі відкритих даних, на подібне обмеження, надання чи оприлюднення такої інформації передбачено законом, обмеження доступу до такої інформації заборонено законом.

У площині останнього розглядається обмеження права на конфіденційність інформації про особу в межах кримінального провадження. Порядок збирання, використання та обробки такої інформації деталізований у Кримінальному процесуальному кодексі України (далі – КПК України). Згідно ст. 162 КПК України персональні дані особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних, відносяться до охоронюваної законом таємниці, яка міститься в речах і документах.

У відповідності до ст. 159, 163 КПК України тимчасовий доступ до речей і документів здійснюється на підставі ухвали слідчого судді, суду. При цьому, слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю, якщо сторона кримінального провадження, доведе можливість використання як доказів відомостей, що містяться в цих речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів [6].

Отже, заходи щодо правової охорони конфіденційної інформації та персональних даних у сфері інформаційних технологій є комплексними та систематичними, де необхідно звертати увагу на

взаємодію приватного та публічного інтересу, що встановлює свій відбиток на протидії різним проявам кіберзлочинності у цій площині з огляду на національне та міжнародне законодавство.

Література:

1. Інформаційні злочини [Електронний ресурс] / Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Інформаційні_злочини.
2. Політанський В.С. Обмеження права на доступ до інформації / В.С. Політанський // Державне будівництво та місцеве самоврядування. – 2013. - № 26. – С. 215-227.
3. Рішення Конституційного суду України “У справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” від 30 жовтня 1997 року № 5-зп. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/v005p710-97/print>.
4. Рішення Конституційного суду України “У справі за поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України” від 20 січня 2012 року № 2-рп/2012. [Електронний ресурс] / Офіційний веб-сайт Верховної Ради України. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/v002p710-12>.
5. Серьогін В.О. Конституційний принцип гласності у діяльності органів державної влади України : автореф. дис. ... канд. юрид. наук : спец. 12.00.02 «Конституційне право» / В.О. Серьогін. – Х., 1999. – 18 с
6. Лист Представника Уповноваженого Верховної Ради України з прав людини від 28 грудня 2015 року № 9-3131/4137-15-73 [Електронний ресурс] / Уповноважений Верховної Ради України. – Режим доступу: <http://www.ombudsman.gov.ua/ua/publication/petition/schodo-pravovix-pidstav-peredachi-personalnix-danix-pravoohoronnim-organam/>.

Теоретико-правові аспекти кіберзлочинності в Україні

Миронець О.М.

старший викладач кафедри конституційного і адміністративного права,
Навчально-науковий Юридичний інститут, Національний авіаційний університет

Колмиков В.В.

студент Навчально-науковий Юридичний інститут
Національний авіаційний університет

У наші дні правопорушення в мережі Інтернет є досить поширеним явищем. Кіберзлочинність у віртуальному просторі становить серйозну загрозу кібербезпеці України, що зумовлює актуальність дослідження її теоретико-правових аспектів.

Віртуальний простір можна визначити як простір, що моделюється за допомогою комп'ютера, інформаційний простір, у якому перебувають відомості про особи, предмети, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [1, с.32-34].

Саме віртуальний простір є сприятливим середовищем для злочинних діянь, які називаються комп'ютерними злочинами або кіберзлочинами.

Кіберзлочинність – це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи вміст кишень пересічних громадян. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців [2].

У наші дні проблема кіберзлочинності набула глобального масштабу, а збитки від діяльності кібершахраїв сягнули десятків мільярдів доларів. Для протистояння кібершахраям в світі створюються спеціальні підрозділи і структури. Їхні повноваження постійно розширюються, а технічні можливості посилюються. Останній приклад – Європейський центр боротьби з кіберзлочинністю, який запрацював на початку 2013 року [3].