Анна Олександрівна Ємельяненко – *студентка І курсу Сумської філії Харківського національного університету внутрішніх справ*
Науковий керівник: **Богдан Іванович Сюркало** – *доцент кафедри юридичних дисциплін Сумської філії Харківського національного університету внутрішніх справ, кандидат економічних наук, доцент*

ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

Захист інформації є однією з одвічних проблем. Протягом всієї історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми – комп'ютерні злочини стали характерною ознакою сьогодення **[**1, 15**]**.

Метою даної публікації є вирішення проблеми та ознайомлення з передумовами виникнення злочинів, що пов’язані з захистом інформації мережі Інтернет. Насамперед, ми маємо знати, що виникнення злочинів, що комп'ютерними називають такі злочини, що пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

Економічні та юридичні питання, національна безпека, приватна та комерційна таємниця – усе це охоплює необхідність захисту інформації та ІС. Згідно із Законом України «Про захист інформації в автоматизованих системах» захист інформації – це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

У літературі ми можемо знайти терміни «безпека інформації» та «безпека інформаційних технологій». Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації. Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити ймовірні загрози,порядок їх настання та можливі наслідки, вибрати надійні засоби і побудувати 100-відстокову систему захисту.

Можемо сказати, що базовими принципами інформаційної безпеки є – забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів **[**2, 128**]**. Із цього погляду основними випадками порушення безпеки інформації можна назвати такі: підробка інформації, блокування інформації; порушення роботи інформаційних систем, несанкціонований доступ; витік інформації; втрата інформації.

Зауважимо, що порушенням безпеки можна вважати і дії, які не призводять безпосередньо до втрати або відпливу інформації, але передбачають втручання в роботу системи.

Щоб детальніше поговорити про захист інформації нам потрібно визначити основні особливості комп'ютерних злочинів: встановлення факту вчинення злочину;відсутність міждержавних кордонів для злочинців (якщо злочин вчиняється з використанням глобальної комп'ютерної мережі).

Нині високотехнологічна злочинність набуває високих темпів. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем. У першому випадку правопорушення можна кваліфікувати за звичайними нормами права (крадіжка, грабіж, розбій і т. ін.). В інших випадках, коли комп'ютер виступає і як інструмент, і як об'єкт, злочин відносять до окремої категорії (див. розділ XVI Кримінального кодексу України).

Правові засоби захисту – чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення,захищають авторські права програмістів та регулюють інші питання використання ІТ. Перехід до інформаційного суспільства вимагає удосконалення карного і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проекту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи), було внесено зміни, оскільки його розцінили як такий, що суперечить положенням про права людини і надає урядам і поліцейським органам зайві повноваження. Загальною тенденцією, що її можна простежити, є підвищення жорсткості кримінальних законів щодо комп'ютерних злочинців. Захист інформації неможливо регламентувати через різноманітність існуючих видів інформації, що обробляється. Конкретні заходи визначаються виробничими, фінансовими та іншими можливостями підприємства (організації), обсягом конфіденційної інформації та її значущістю.

Таким чином, правові основи захисту в мережі Інтернет – це чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією. Порушенням безпеки можна вважати дії, які не призводять безпосередньо до втрати або відпливу інформації, але

передбачають втручання в роботу системи. На кожний комп'ютерний злочин ми маємо свою протидію.

Література

1. Макарова М.В. Електронна комерція: Посібник для студ. вищих навчальних закладів. – К.: Видавничий центр "Академія", 2002. – 272 с.
2. Балабанов И.Т. Электронная коммерция. – СПб.: Питер, 2001. – 336 с.

Сергій Олександрович Жировий – *студент IV курсу Національного юридичного університету імені Ярослава Мудрого*
Науковий керівник: **Володимир Анатолійович Гуменюк** *– головний спеціаліст відділу Харківського апеляційного адміністративного суду, кандидат юридичних наук, доцент*

ДЕЯКІ ПРОБЛЕМИ РЕАЛІЗАЦІЇ ДОКАЗІВ У АДМІНІСТРАТИВНОМУ ПРОЦЕСІ

Незважаючи на те, що поняття доказів нормативно закріплено, питання визначення доказів, їх видів залишається одним з найбільш суперечливих.

Так, при розгляді справ про адміністративні правопорушення, орган (посадова особа) зобов'язаний з'ясувати, чи було вчинено адміністративне правопорушення, чи підлягає особа адміністративній відповідальності, а також інші обставини, що мають значення для правильного вирішення справи. У даному випадку в основу покладені положення Кодексу України про адміністративні правопорушення (далі – КУпАП), зокрема ст. 251. Однак, суд при вирішенні спорів між фізичними особами та суб'єктами владних повноважень щодо оскарження рішень останніх – постанов у справах про адміністративні правопорушення керується нормами Кодексу адміністративного судочинства України (далі – КАС України). Спробуємо розглянути існуючі питання колізії встановлення фактичних даних (доказів) при прийнятті рішення у справі про адміністративне правопорушення та його оскарження у адміністративному суді.

У ст. 251 КУпАП зазначено, що доказами у справі про адміністративне правопорушення, є будь-які фактичні дані, на основі яких у визначеному законом порядку орган (посадова особа) встановлює наявність чи відсутність адміністративного правопорушення, винність даної особи в його вчиненні та інші обставини, що мають значення для правильного вирішення справи [1]. В той же час, КАС України у ст. 72 говорить про те, що доказами в адміністративному судочинстві є будь-які