

Дімітрова Наталія Миколаївна

Миколаївський інститут права

Національного університету «Одеська юридична академія»

Білик Наталя Михайлівна

Кандидат технічних наук, доцент

Миколаївський інститут права

Національного університету «Одеська юридична академія»

ОСНОВНІ ВИДИ КІБЕРЗЛОЧИНІВ ТА ПРИЧИНИ, ЩО ЇХ ПОРОДЖУЮТЬ

На сьогодні комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. На відміну від традиційних видів злочинів, історія яких налічує століття, таких як вбивство або крадіжка, кіберзлочинність явище відносно молоде і нове, яке виникло з появою мережі Інтернет. Специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, практично не відходячи від «робочого місця», злочини є доступними, оскільки комп'ютерна техніка постійно дешевшає, злочини можна скоювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців.

Отож розглянемо причини, що породжують кіберзлочинність, та фактори що на неї впливають:

Першою причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова. Величезні суми грошей з'являються в кишенях злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть просто потоком.

Друга причина росту кіберзлочинності як бізнесу – те, що успіх справи не пов'язаний з великим ризиком. У реальному світі психологічний аспект злочину припускає наявність деяких факторів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше.

Основні види кіберзлочинів:

порушення авторського права і суміжних прав; шахрайство; ухилення від сплати податків, зборів (обов'язкових платежів); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ввезення, виготовлення, збут і розповсюдження порнографічних предметів; незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю.

Таким чином, кіберзлочинність – це проблема, з якою зіштовхнулась планета у ХХІ столітті, і яка обіцяє рости та поглинати все більше коштів. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

Отже, міжнародне співробітництво є ключовим моментом у подоланні та протидії кіберзлочинності у глобальних інформаційних мережах, а також причин що їх породжують. Однак, єдиним шляхом подолання і забезпечення особистої безпеки користувачів від електронних посягань, полягає в дотриманні правил користування Інтернет ресурсами, створення надійних паролів, захист особистої інформації, встановлення антивірусних програм та використання захищених мереж.