

**Ю.Є. Добришин**

*кандидат технічних наук, доцент,  
Навчально-науковий інститут комп'ютерних та інформаційних технологій  
Університет економіки та права «КРОК»*

**В.В. Семенов**

*кандидат юридичних наук, доцент кафедри кримінально-правових ННПП  
Національної академії внутрішніх справ*

### **Криміналістичне забезпечення розслідування комп'ютерних злочинів**

У статті розглянуто проблемні питання щодо створення у відомчих установах сучасної кадрової, методичної і матеріально-технічної бази підготовки і перепідготовки фахівців з розслідування комп'ютерних злочинів

**Ключові слова:** комп'ютерна злочинність, підготовка кадрів, інформаційне середовище, криміналістичне забезпечення, професійні якості.

#### ***Основний текст***

У зв'язку з відносною новизною комп'ютерної злочинності не можна не виділити серед основних напрямів організації її протидії необхідність створення ефективної системи професійної підготовки кадрів.

Одним із основних завдань даного напрямку, є створення у відомчих установах сучасної кадрової, методичної і матеріально-технічної бази підготовки і перепідготовки потрібних фахівців. Система підготовки кадрів повинна підкріплюватися науковими дослідженнями відповідного профілю.

Розвиток подібної системи повинен не тільки виходити з вимог сьогодення, але і враховувати тенденції зміни злочинності в майбутньому. Формування кадрового ядра спеціалізованих підрозділів правоохоронних органів повинне включати три важливі напрями: професійну підготовку, перепідготовку і підвищення кваліфікації їх співробітників. При цьому особливу увагу слід приділяти останньому напрямку: кожен працівник, який залучений до діяльності в даному напрямку повинен регулярно проходити навчання, з тим щоб бути в курсі новацій у сфері технологій і юридичної практики, що склалася.

Комплекс необхідних професійних якостей осіб, задіяних по лінії боротьби із комп'ютерною злочинністю, крім звичайних (надійність, компетентність і професіоналізм, добре розвинена пам'ять, схильність до аналізу, пунктуальність і т. д.), повинен включати деякі додаткові

вимоги. Наприклад, такі як:

- навички спілкування в «комп'ютерних» колах, розуміння особливостей цього середовища, володіння лексикою що використовується в ньому;
- знання сучасних операційних систем;
- розуміння механізмів злому комп'ютерних систем і відповідних методів протидії;
- уміння читати і аналізувати складні системні файли (журнали реєстрації подій, файли настройки конфігурації і т. п.), виконувати аналітичний пошук кореляції між подіями або сигнатурами нападу, визначати тип загрози;
- володіння апаратними і програмними засобами фіксації отриманої інформації і виявлення підозрілих подій;
- уміння доступно висловлювати в документах і усно складну технічну інформацію.

Для розуміння явищ, що відбуваються в інформаційному середовищі, все частіше потрібні глибокі знання самих різних аспектів функціонування сучасного суспільства. До аналітичної роботи необхідно залучати фахівців з різносторонньою підготовкою. Вони повинні бути здатні враховувати різноманітні чинники мотивації комп'ютерних злочинів, бути досвідчені в різних сферах (технічної, економічної, соціальної, юридичної і ін.).

Недостатній рівень теоретичної і практичної підготовки співробітників правоохоронних органів в даній сфері пов'язаний і із слабкою забезпеченістю науковими дослідженнями відповідного профілю. В зв'язку з цим представляється перспективною організація спеціалізованих структур із проблем комп'ютерної злочинності, завданням яких є вивчення, розробка стратегічних і тактичних підходів до розкриття комп'ютерних злочинів на основі комплексного вивчення тенденцій комп'ютерних кримінальних процесів. Безперечно користь могло б принести створення центру аналізу комп'ютерних злочинів, покликаною здійснювати аналітичну і методичну діяльність, інформування громадськості про загрози, які несе комп'ютерна злочинність, а також розроблення методів профілактики.

Не менш складну проблему становить недостатня забезпеченість спеціалізованих підрозділів засобами обчислювальної техніки, спеціальними приладами і устаткуванням. Тим часом від такої оснащеності залежить не тільки результативність розслідувань, що провадяться, але і, що не менш важливо, якість криміналістичних експертиз, пов'язаних з аналізом доказів в електронному вигляді. Подібні експертизи нерідко пов'язані з необхідністю аналізу справді гігантських об'ємів комп'ютерних даних.

Ефективність науково-дослідних робіт, направлених на попередження та розслідування комп'ютерних злочинів, також багато в чому визначається рівнем забезпеченості технічними засобами та програмними продуктами. І безумовно, технічне оснащення безпосередньо визначається фінансовими вкладеннями в цю сферу.

Підводячи підсумок викладеному, необхідно ще раз підкреслити, що підвищення ефективності боротьби із комп'ютерною злочинністю безпосередньо пов'язано з комплексним рішенням означених проблем. І можна констатувати, що передумови для цього є, оскільки теорією в основному вироблені, а практикою постійно удосконалюються відповідні рекомендації в даній сфері.