1. Комп'ютерні злочини це одна з найдинамічних груп суспільно-небезпечних посягань у структурі загально-кримінальної та транснаціональної злочинності.

2. Криміналістична особливість кіберзлочинів полягає в тому, що їх розкриття не можливе без застосування та використання комп'ютерних технологій. Особливо гостро постає проблема збирання доказів в електронній формі при виконанні оперативно-розшукових заходів у сфері протидії кіберзлочинності.

3. Сучасні кіберзлочинці є представниками новітньої цифрової доби та характеризуються підвищеним рівнем обізнаності у сфері інформаційно-телекомунікаційних систем, що ускладнює розкриття цих злочинів.

4. Основними недоліками у протидії кіберзлочинності є неузгодженість нормативно-правових актів стосовно процедури проведення та кадрового потенціалу експертів для проведення комп'ютерно-технічних експертиз в цій сфері.

5. Однією із нагальних проблем кадрового забезпечення підрозділів кримінальної поліції Національної поліції України є нестача ІТ-спеціалістів, за рахунок: недостатньої інформаційно-технологічної спеціалізованої підготовки оновленого складу підрозділів кіберполіції, низького матеріально-технічного оснащення оперативних підрозділів кіберполіції, неврегульованості процесуальної взаємодії між національними та міжнародними поліцейськими структурами в світлі вимог Конвенції про боротьбу з кіберзлочинністю.

**Література:**

1. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю / О.В. Орлов, Ю.М. Онищенко // Теорія та практика державного управління.-2013.- Вип. 3. – С 3-9. – Режим доступу: http://gov.ua/j-pdf/Tpdu_2013_3_3.pdf

2. 2015 Internet Securit Threat Report [ Електронний ресурс ]. –Режим доступу: http://www.symantec.com/security_respons/publication/ whitepapers.jsp

3. В тенетах світової павутини: тенденції розвитку кібербезпеки у 2016 році // [Електронний ресурс]. Режим доступу: http://defence-ua.com/index.php/statti/

## Загальна методика експертної оцінки рівнів захищеності інтегрованих інформаційних систем МВС України

**Кудінов В.А.**
кандидат фізико-математичних наук, доцент,
професор кафедри інформаційних технологій та кібернетичної
безпеки Національної академії внутрішніх справ

Серед основних напрямів державної інформаційної політики в Україні сьогодні, відповідно до ст. 3 Закону України «Про інформацію», є створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України. Тому останнім часом в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій практично у всі сфери життєдіяльності держави, у тому числі в діяльність органів та підрозділів Національної поліції, МВС України.

В МВС України вже протягом більше 45 років накопичено чималий досвід використання різноманітних інтегрованих інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення. Департаментом інформаційних технологій МВС України створена та постійно удосконалюється система інформаційного забезпечення, яка здійснює інформаційну підтримку діяльності органів та підрозділів Національної поліції щодо забезпечення запобігання кримінальним правопорушенням, їх виявлення, припинення, розкриття і розслідування, розшуку осіб, які вчинили кримінальні правопорушення, надає багатоцільову статистичну, аналітичну та довідкову інформацію, допомагає при розв'язані інших завдань боротьби зі злочинністю.

Одним з важливих напрямів ефективного функціонування інтегрованих інформаційних систем МВС України є забезпечення їх захищеності.

Побудова комплексної системи захисту інформації (далі – КСЗІ) в цих системах повинно дозволити запобігти або ускладнити можливість реалізації загроз порушення цілісності, доступності та конфіденційності інформації, а також належного функціонування ресурсів з її обробки, знизити

потенційні збитки у разі їх здійснення, локалізацію та ліквідацію наслідків їх впливу [2; 3]. Враховуючи трьохрівневу ієрархічну модель організації функціонування багатьох інтегрованих інформаційних систем МВС України, КСЗІ повинна забезпечити на кожному їх структурному рівні функціонування інформаційних систем класу «2», а функціонування в цілому – як інформаційної системи класу «3» [4]. Тобто, побудова КСЗІ в інтегрованих інформаційних системах МВС України передбачає об'єднання в єдину систему всіх необхідних заходів та засобів захисту від різних загроз безпеці інформації на всіх етапах її життєвого циклу [2; 5; 6].

Розглянемо загальну методику експертної оцінки рівнів захищеності інтегрованих інформаційних систем МВС України.

*По-перше,* необхідно виділити найбільш вірогідні об'єкти обробки інформації в них з порушенням її цілісності, доступності та конфіденційності.

*По-друге,* необхідно розглянути модель імовірного порушника безпеки для вибраних об'єктів захисту, яка оцінює не тільки самого порушника, але також визначає загрози цим об'єктам. У роботі [7] наведена загальна модель імовірного порушника безпеки та у якості базових моделей захисту інформації розглянуто найпростіші моделі пасивного й активного каналів витоку інформації, моделі ненавмисного і навмисного несанкціонованого доступу.

*По-третє*, необхідно виділити всі існуючи засоби та заходи захисту для вибраних об'єктів захисту. У роботі [2] запропоновано комплекс основних заходів захисту апаратно-технічних засобів та програмного забезпечення з обробки інформації.

*По-четверте*, необхідно здійснити на основі досвіду фахівців з захисту інформації експертну оцінку ймовірності подолання існуючих засобів та заходів захисту (далі – події) $P_{под}$ для вибраних об'єктів захисту, значення якої визначається в межах від 0 до 1. З метою створення єдиного підходу до оцінки $P_{под}$ пропонується ввести таку шкалу її значень:

1) $P_{под} = 0$, якщо подія неможлива;
2) $P_{под} = 0{,}2$, якщо низка ймовірність події;
3) $P_{под} = 0{,}5$, якщо ймовірності появи події та її відсутності однакові;
4) $P_{под} = 0{,}8$, якщо висока ймовірність події;
5) $P_{под} = 1$, якщо подія відбудеться обов'язково.

Необхідно зазначити наступне: а) якщо для об'єкту захисту існує низка шляхів подолання існуючих засобів та заходів захисту з різними значеннями $P_{под}$, то у підсумковій експертній оцінці необхідно брати її найбільше значення; б) якщо для об'єкту захисту існує низка засобів та заходів захисту від конкретного впливу порушника безпеки з різними значеннями $P_{под}$, то у підсумковій експертній оцінці необхідно брати її найменше значення.

Таким чином, використання цієї загальної методики дозволяє отримати цифрові дані щодо рівнів захищеності інтегрованих інформаційних систем МВС України.

Наведена загальна методика експертної оцінки рівнів захищеності інтегрованих інформаційних систем МВС України (на підставі експертної оцінки ймовірності подолання засобів та заходів захисту інформації та ресурсів з її обробки) дозволяє провести для кожної з них всебічний аналіз комплексної системи захисту інформації та виявити в ній слабкі ланки, які потребують подальшого удосконалення.

**Література:**

1. Про інформацію: Закон України від 02 жовтня 1992 року № 2657-XII. *Верховна Рада України*. URL: http://zakon3.rada.gov.ua/laws/show/2657-12.

2. Кудінов В. А. Організація комплексу заходів захисту апаратно-технічних засобів та програмного забезпечення системи оперативного інформування МВС України / В. А. Кудінов // Сучасна спеціальна техніка. – 2011. – № 4. – С. 54-59.

3. Кудінов В. А. Оцінка ефективності комплексної системи захисту інформації в системі оперативного інформування МВС України / В. А. Кудінов // Сучасна спеціальна техніка. – 2011. – № 1. – С. 91-96.

4. Кудінов В. А. Напрями подальшого розвитку методології оцінки рівнів захищеності інтегрованої інформаційно-телекомунікаційної системи оперативного інформування МВС України у зв'язку з набуттям чинності нового КПК України / В. А. Кудінов // Сучасна спеціальна техніка. – 2013. – № 1. – С. 126-130.

5. Кудінов В. А. Аналіз загальних особливостей функціонування основних об'єктів інформаційної безпеки інтегрованих інформаційних систем органів внутрішніх справ України / В. А. Кудінов // Сучасна спеціальна техніка. – 2012. – № 1. – С. 91-96.

6. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 року № 22.

7. Кудінов В. А. Корпоративна мережа ОВС України та моделі її захисту від порушників безпеки / В. А. Кудінов, В. О. Хорошко // Захист інформації. – 2004. – № 1. – С. 26-35.

## Початок досудового розслідування кримінальних проваджень, пов'язаних із незаконним розповсюдженням медійного контенту в мережах провайдерів програмної послуги та Інтернет-провайдерів мережі Інтернет

**Кунтій А.І.**
кандидат юридичних наук
доцент кафедри кримінального процесу
факультету №1 ІПФПНП Львівськог державного
университету внутрішніх справ

Сучасний медіапростір характеризується стрімким розвитком, появою нових способів поширення інформації, необмеженим доступом до останньої, що, в свою чергу, не могло не позначитись на сфері регулювання цього простору. Технологічний прогрес, що відбувається сьогодень, має чимало позитиву, проте, нажаль, Інтернет простір став ще одним способом учинення різноманітних злочинів. Сьогодні саме в мережі Інтернет зосереджена основна частина медіа контенту, проте його безконтрольне поширення завдає чималої шкоди різним сферам життєдіяльності людини.

Незаконне розповсюдження медійного контенту є способом вчинення злочинів, що посягають на різні об'єкти, які знаходяться під кримінально правовою охороною. Найпоширенішими видами порушень в мережі Інтернет є: незаконне відтворення і копіювання музичних, художніх, літературних творів чи комп'ютерних програм без попереднього надання на це згоди автором чи правовласником. Це виражає порушення матеріальних прав авторів.

Питанням пов'язаних з розслідуванням порушенням авторського та суміжних прав Т.В. Авер'янова, В.П. Бахін, Р.С. Бєлкін, П.Д. Біленчук, В.Б. Вєхов, А.Ю. Головін, В.О. Голубєв, В.Г. Гончаренко, В.А. Журавель, А.В. Іщенко, О.Н. Колесніченко, В.К. Лисиченко, І.М. Лузгін, Г.А. Матусовський, Б.В. Романюк, М.В. Салтевський, М.Я. Сегай, В.В. Тіщенко, В.Ю. Шепітько та інші.

Крім цього, все популярніше стає такий вид порушень як плагіат. Такі порушення в мережі Інтернет порушують матеріальні і нематеріальні права авторів. За офіційними даними у 2015 році було зареєстровано 250 фактів порушення авторських та суміжних прав; у 2016 році - 157; протягом січня-серпня 2017 року – 78 [1].

Незаконне розповсюдження медійного контенту в мережі Інтернет характеризується високим рівнем латентності, що, як зазначають науковці, пов'язане із особливостями функціонування Інтернету, а саме: анонімності користувачів, екстериторіального характеру, свобод та швидкості поширення інформації – порушення авторських прав стало настільки буденним і поширеним явищем, що особа, вчиняючи протиправні дії, просто не усвідомлює їх сутності, а навпаки гадає, що діє в рамках закону [2].

Під «медійним контентом» в ході нашого дослідження ми розуміємо «матеріали» тобто будь-яку інформацію, яка може передаватися з використанням мережі Інтернет, або через засобів масової інформації. Згідно ч.2 ст. 22 ЗУ від 2.10.1992 р. «Про інформацію» засобами масової інформації (ЗМУ) є засоби, призначені для публічного поширення друкованої або аудіо-візуальної інформації. Такими можуть бути провайдери програмної послуги та Інтернет-провайдерів мережі Інтернет.

Узагальненням нами слідчо-судової практики свідчить про те, що досудове розслідування у кримінальних провадженнях досліджуваної категорії може бути розпочате:

- на підставі заяви, повідомлення окремих громадян чи юридичних осіб;
- із самостійного виявлення ознак кримінального правопорушення працівниками правоохоронних органів;
- під час розслідування іншого кримінального провадження.

В разі надходження до органів поліції заяв, повідомлень про злочини, пов'язані із незаконним розповсюдженням медійного контенту в мережах провайдерів програмної послуги та Інтернет-провайдерів мережі Інтернет, уповноважена службова особа, зобов'язана зареєструвати таку заяву (повідомлення) до журналу ЄО і після цього слідчий, прокурор зобов'язані перевірити таку заяву (повідомлення) чи містить таке ознаки кримінального правопорушення, негайно, але не пізніше 24 год.