Міністерство внутрішніх справ України
Харківський національний університет внутрішніх справ

КРАВЦОВА МАРИНА ОЛЕКСАНДРІВНА

УДК 343.85

КІБЕРЗЛОЧИННІСТЬ: КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА ТА ЗАПОБІГАННЯ ОРГАНАМИ ВНУТРІШНІХ СПРАВ

12.00.08 – кримінальне право та кримінологія;
кримінально-виконавче право

Автореферат
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Харків – 2016

Дисертацією є рукопис

Робота виконана у Харківському національному університеті внутрішніх справ, Міністерство внутрішніх справ України.

Науковий керівник – доктор юридичних наук, професор **Литвинов Олексій Миколайович,** Харківський національний університет внутрішніх справ, завідувач кафедри кримінального права та кримінології факультету № 1;

Офіційні опоненти: доктор юридичних наук, професор **Карчевський Микола Віталійович,** Луганський державний університет внутрішніх справ імені Е. О. Дідоренка, проректор;

кандидат юридичних наук, доцент **Сингаївська Інна Володимирівна,** Національний університет державної податкової служби України, доцент кафедри кримінального права та кримінології.

Захист відбудеться 7 квітня 2016 року о 09.00 годині на засіданні спеціалізованої вченої ради Д 64.700.03 у Харківському національному університеті внутрішніх справ (61080, м. Харків, пр-т Лева Ландау, 27).

З дисертацією можна ознайомитись у бібліотеці Харківського національного університету внутрішніх справ (61080, м. Харків, пр-т Лева Ландау, 27).

Автореферат розісланий 4 березня 2016 року.

Вчений секретар
спеціалізованої вченої ради **Д. Ю. Кондратов**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Органи внутрішніх справ (далі – ОВС) України традиційно розглядалися в числі ключових спеціалізованих суб'єктів протидії злочинності. Втім, логіка історичного процесу на початку XXI ст. змусила переглянути базові підходи до стратегії державного будівництва і загальносоціального розвитку в цілому Це не могло не позначитись на системі кримінальної превенції, в структурі якої, згідно Закону України «Про Національну поліцію» від 02.07.2015 року, сформовано новий орган – Національну поліцію. Маючи в основі своєї діяльності сервісну, людиноцентристську концепцію, поліція концентровано увібрала в себе основне функціональне навантаження ОВС, в тому числі й у напрямі протидії злочинності. Однак, вести мову про цілковитий перехід превентивної функції від ОВС до поліції не доводиться: вказаний Закон визначив координуючу, інформаційно-аналітичну роль МВС по відношенню до діяльності Національної поліції, що обґрунтовує доцільність дослідження синтетичних форм їх кримінологічної практики. Чимале значення в належній організації цього напряму роботи ОВС та поліції має її наукове кримінологічне супроводження. Однак останнє виявляє недостатню адаптивність до новітніх соціальних викликів щодо запобігання окремим різновидам злочинності, зокрема й кіберзлочинності.

Комп'ютерні технології стали невід'ємною складовою розвитку виробничих відносин та особистісних комунікацій. Виникнення, розширення, ускладнення віртуальної реальності не могло залишитись осторонь загальних закономірностей соціодинаміки, іманентною складовою яких традиційно визнається злочинність. Системна цілісність та, водночас, багатогранність суспільного життя з об'єктивною необхідністю зумовила відтворення кримінальної активності й у тих сферах, які позначились найбільш інтенсивним використанням комп'ютерних технологій, можливостей електронних мереж. Наразі є достатні підстави вести мову про існування феномену кіберзлочинності (комп'ютерної злочинності).

Про небезпечність цього феномену свідчать положення Закону України «Про основи національної безпеки України» від 19.06.2003 року, ст. 7 якого визнає комп'ютерну злочинність та комп'ютерний тероризм загрозами національним інтересам і національній безпеці країни в інформаційній сфері. Згідно зі ст. 1 Закону України «Про боротьбу з тероризмом» від 20.04.2003 року технологічний тероризм, як злочин, що вчиняється з терористичною метою із застосуванням комп'ютерних систем і комунікаційних мереж, створює умови для аварій і катастроф техногенного характеру. Втім, у фокусі кібернетичних загроз перебувають не лише відносини у сфері національної безпеки, а й ті з них, на яких ґрунтується буденна життєдіяльність громадян: у сфері власності, громадського порядку й моральності, службової діяльності тощо.

Також слід зауважити, що масштаб позначеної проблеми не обмежується кордонами однієї держави, адже сучасні глобальні комп'ютерні мережі охоплюють переважну більшість країн світу, що додатково актуалізує цілий пласт науково-прикладних аспектів протидії транснаціональній злочинності. Різке підвищення кримінального комп'ютерного професіоналізму, висока мобільність злочинців, їх організованість здатні виступати чинниками дестабілізації криміногенної

обстановки в державі, регіоні та світі. Це ставить на порядок денний питання про необхідність адекватної, системної, узгодженої, випереджаючої реакції правоохоронних органів на швидкозмінні високотехнологічні кримінально-кібернетичні загрози. Основними суб'єктами розгортання та нарощування такої реакції є ОВС та Національна поліція.

Дослідженню феномену, проявів, детермінант, питанням запобігання кіберзлочинності присвячено чимало наукових праць вітчизняних і зарубіжних фахівців у галузі кримінального права, кримінології, криміналістики, психології, а також дослідників із суміжних сфер: кібернетики, інформатики тощо. Зокрема, цій проблематиці присвячені роботи Д. С. Азарова, О. А. Баранова, Ю. М. Батуріна, П. Д. Біленчука, В. В. Василевича, А. А. Васильєва, В. Д. Гавловського, В. О. Глушкова, В. О. Голубєва, Н. О. Гуторової, Р. А. Калюжного, М. В. Карчевського, М. М. Коваленка, М. Й. Коржанського, В. В. Крилова, Ю. І. Ляпунова, П. С. Матишевського, М. І. Мельника, А. А. Музики, В. О. Навроцького, П. І. Орлова, С. О. Орлова, М. І. Панова, Д. В. Пашнєва, А. О. Пінаєва, Н. А. Розенфельд, В. В. Сташиса, Є. Л. Стрельцова, В. Я. Тація, В. П. Тихого, В. М. Трубникова, М. І. Хавронюка, В. Б. Харченка, В. С. Цимбалюка, Н. М. Ярмиш та інших. Однак, не дивлячись на наявність значного масиву напрацювань з означеного напряму наукового пошуку, слід зауважити, що монографічного дослідження, присвяченого розробці науково обґрунтованої системи заходів запобігання кіберзлочинності на основі її сучасної кримінологічної характеристики й досі не здійснено.

Викладені обставини у своїй сукупності обґрунтовують актуальність теми дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційного дослідження відповідає п. 5.16 додатку 5 до Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 років (затвердженого Наказом МВС України від 16.03.2015 року № 275), п. 5.2 Пріоритетних напрямів наукових досліджень Харківського національного університету внутрішніх справ на період 2016–2019 років, а також комплексній темі наукових досліджень кафедри кримінального права та кримінології факультету № 1 Харківського національного університету внутрішніх справ на 2014–2018 роки «Протидія злочинності кримінально-правовими та кримінологічними засобами» (номер державної реєстрації 0113U008195).

Тему дисертації затверджено Вченою радою Харківського національного університету внутрішніх справ 23.02.2012 року (протокол № 2).

Мета та задачі дослідження. *Метою* дослідження є формування комплексної кримінологічної характеристики кіберзлочинності та вироблення на цій основі науково обґрунтованих рекомендацій щодо запобігання цим злочинам ОВС та Національною поліцією.

Для досягнення поставленої мети необхідно вирішити такі *задачі*:

– визначити поняття кіберзлочинності, з'ясувати її феномен та прояви;

– здійснити кримінологічну класифікацію кіберзлочинів;

– охарактеризувати сучасний стан кіберзлочинності в Україні через опис і пояснення її кількісних та якісних кримінологічних показників;

– надати характеристику особистості кіберзлочинця, визначити її специфічні риси;

– дослідити особливості детермінації кіберзлочинності;

– охарактеризувати правові засади запобігання кіберзлочинності ОВС і Національною поліцією;

– визначити та описати систему заходів запобігання кіберзлочинності ОВС і Національною поліцією, виробити пропозиції щодо її удосконалення;

– дослідити наукові засади та прикладні аспекти взаємодії ОВС і Національної поліції з іншими суб'єктами запобігання кіберзлочинності та запропонувати, на цій підставі, шляхи її оптимізації.

Об'єктом дослідження є суспільні відносини у сфері забезпечення кібернетичної складової кримінологічної безпеки України.

Предметом дослідження є кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ.

Методи дослідження. Методологічну основу дисертаційного дослідження на філософському рівні пізнання склали основні принципи та категорії діалектичного детермінізму. На загальнонауковому – формально-логічні методи, як-от: гіпотеза, аналіз, синтез, індукція, дедукція, порівняння та інші. Спеціально-науковий рівень репрезентований статистичними, конкретно-соціологічними, психологічними методами дослідження.

Філософія діалектичного детермінізму забезпечила системність у вивченні феномену та проявів кіберзлочинності, її історично закономірної природи (підрозділ 1.1), розгалужених детермінаційних зв'язків як частини цілісного й суперечливого процесу соціодинаміки (підрозділ 2.2). Формально-логічні методи використовувались при конструюванні композиції дослідження в цілому та за окремими розділами, а також при аналізі, поясненні, кримінологічній інтерпретацій емпіричних даних щодо стану, детермінант кіберзлочинності, особистості кіберзлочинця, системи необхідних та доцільних заходів запобігання (підрозділи 1.2, 2.1, 2.2, 3.2). Порівняльно-правовий метод застосовано при дослідженні відповідності положень національного законодавства України нормам міжнародного права у сфері запобігання кіберзлочинності (підрозділи 1.1, 3.1). В результаті застосування статистичних методів досліджено показники рівня, структури та динаміки кіберзлочинності (підрозділ 1.2). Методи групування, системно-структурний і структурно-функціонального аналізу застосовано для дослідження детермінаційного комплексу кіберзлочинності та системи запобігання цьому явищу (підрозділи 2.2, 3.1–3.3). Конкретно-соціологічні методи (невключене соціологічне спостереження, експертні оцінки, контент-аналіз) використані для аналітичного опрацювання матеріалів кримінальних справ і проваджень, виявлення рівня латентності кіберзлочинів, особливостей механізму їх вчинення та детермінації, стану, проблем та перспектив розвитку взаємодії ОВС й Національної поліції з іншими суб'єктами запобігання кіберзлочинності (підрозділи 1.2, 2.1, 2.2, 3.2, 3.3).

Правову основу дисертації складають Конституція України, міжнародні договори, ратифіковані Верховною Радою України, нормативно-правові акти

Верховної Ради України, Президента України, Кабінету Міністрів України, МВС, СБУ, інші чинні нормативно-правові акти.

Емпіричну базу дисертаційного дослідження склали: 1) дані офіційної статистичної звітності МВС України за 2002–2012 рр.; 2) дані офіційної статистичної звітності Генеральної прокуратури України за 2013–2015 рр.; 3) дані офіційної статистичної звітності Державної судової адміністрації України за 2004–2015 рр.; 4) матеріали 150 архівних кримінальних справ та проваджень, за якими винесено обвинувальні вироки та засуджено осіб за вчинення злочинів, передбачених за ст.ст. 361–363-1 КК України; 5) експертні оцінки 25 фахівців вітчизняних ІТ-компаній, 37 спеціалістів у сфері захисту інформації та правоохоронної діяльності.

Наукова новизна одержаних результатів полягає у тому, що дисертація є першим в Україні монографічним дослідженням, в якому надана комплексна кримінологічна характеристика кіберзлочинності, вироблена система заходів запобігання її поширенню ОВС та Національною поліцією. Основні положення, які складають наукову новизну, полягають в тому, що:

вперше:

– надано комплексну кримінологічну характеристику кіберзлочинності, в результаті чого встановлено її високий рівень, несприятливу динаміку з тенденцією до позитивного приросту, високу латентність, ускладнену груповими формами кримінальної активності, а також рецидивом злочинів, структуру, залежну від чинника урбанізації географію;

– здійснено комплексну класифікацію кіберзлочинів фасетним способом, в результаті чого на підставі 8 критеріїв (особистісних рис злочинця, мотивів злочину, особливостей механізму злочинної та віктимної поведінки, організованості, епізодичності злочинної діяльності, а також залежно від наявності чи відсутності рецидиву злочинів і їх технологічної складової) виділено 61 їх різновид;

– надано кримінологічну характеристику особистості кіберзлочинця, в результаті чого встановлено, що в більшості своїй – це працездатні, але не працюючі (43,7 %), неодружені (58 %), одружені, але такі, що з родиною не живуть – 16 %), чоловіки (90,8 %), віком 30–50 років (43,1 %), громадяни України (95,5 %), які мають вищу освіту (48,1 %), в структурі морально-психологічних якостей яких превалюють корисливість, правовий нігілізм, поєднані з детермінованим специфікою кіберпростору комплексом сваволі та ілюзій;

удосконалено:

– поняття кіберзлочинності, під якою запропоновано розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп’ютерів), телекомунікаційних систем, комп’ютерних мереж і мереж електрозв’язку;

– систему заходів запобігання кіберзлочинності ОВС та Національною поліцією, яка включає превентивну діяльність на спеціально-кримінологічному та індивідуальному рівнях, передбачає концептуально цілісний, узгоджений та керований вплив на детермінаційний комплекс кіберзлочинності з урахуванням специфіки внутрішньодержавних суспільних протиріч, а також потреб у реагуванні

на швидкозмінні фактори розвитку комп'ютерних технологій, прояви зовнішньої агресії по відношенню до України, яка розгортається в тому числі й у кіберпросторі, в результаті чого запропоновано: а) формування та ведення оперативних й профілактичних обліків суб'єктів підвищеного кіберкриміногенного ризику; б) посилення контролю за виготовленням, виробництвом, ввезенням на територію України (вивезенням з неї), переміщенням, зберіганням, збутом технічних засобів збирання, зберігання, обробки, передачі інформації, заборонених або обмежених у цивільному обігу; в) заходи з активізації превентивної діяльності щодо виявлення осіб, схильних до вчинення кіберзлочинів, запобігання й припинення їх кримінальної активності; г) заходи з приєднання до міжнародних програм і технологічних систем запобігання кіберзлочинам тощо;

– обґрунтування кримінально-правового обсягу поняття «кіберзлочинність», який визначається злочинами, передбаченими ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України; їх кримінологічно значущу, предметно-діяльнісну природу складає не тільки і не стільки особлива сфера суспільних відносин (щодо використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку), скільки їх віртуалізована частина, переміщена до кіберпростору та функціонально спрямована на забезпечення нормального стану суспільних відносин іншого роду – власності, господарської, службової діяльності тощо;

дістало подальшого розвитку:

– наукове положення про комплекс взаємодіючих і взаємообумовлених політико-правових, соціально-економічних, організаційно-управлінських та культурно-психологічних факторів детермінації кіберзлочинності; доведено, що особливості детермінації кіберзлочинності обумовлені інформаційно-технологічними властивостями кіберпростору як специфічного середовища формування особистості злочинця у його взаємозв'язку з відповідними об'єктивними чинниками макро- та макрорівня соціальних взаємодій;

– пояснення причин різкого зростання кіберзлочинності в Україні протягом 2013–2015 рр., серед яких чільне місце посідають правові, економічні, соціальні чинники, а також кібернетична складова зовнішньої агресії по відношенню до нашої держави, що підкріплюється внутрішньою підривною діяльністю окремих груп кіберзлочинців;

– характеристика правових засад запобігання кіберзлочинності з урахуванням основного функціонального кримінально-превентивного навантаження на Національну поліцію під координуючим началом та інформаційно-аналітичним забезпеченням МВС, в результаті чого виявлено та описано системно-правові зв'язки в механізмі правового регулювання їх діяльності, окремі їх недоліки (прогалини) та шляхи усунення; наведено додаткові аргументи на користь необхідності прийняття Закону України «Про органи внутрішніх справ»;

– наукові засади та прикладні аспекти взаємодії ОВС та Національної поліції з іншими суб'єктами запобігання кіберзлочинності, під якою запропоновано розуміти засновану на чинному законодавстві, узгоджену за метою, завданнями, місцем і часом, компетенцією, можливостями, спільну та доцільну, багатоваріативну й різноспрямовану діяльність спеціалізованих і неспеціалізованих суб'єктів

кримінальної превенції як на національному, так і міжнародному рівнях.

Практичне значення одержаних результатів полягає в тому, що висновки та пропозиції, які містяться у дисертації, можуть бути використані:

– у науково-дослідній сфері – для подальшої розробки наукових положень про феномен кіберзлочинності, його детермінанти, особливості проявів (Акт впровадження результатів дисертаційного дослідження у діяльність Кримінологічної асоціації України від 28 серпня 2015 року);

– у правотворчості – для надання пропозицій із вдосконалення відомчих нормативно-правових актів Національної поліції щодо запобігання кіберзлочинам;

– у правозастосовній діяльності – для надання пропозицій із вдосконалення напрямів діяльності ОВС, Національної поліції щодо запобігання кіберзлочинам, а також для інформування громадян щодо вжиття заходів активної віктимологічної профілактики;

– у навчальному процесі – при викладанні курсів «Кримінологія», «Кримінологія та профілактика злочинів», а також похідних від них спеціальних курсів у вищих навчальних закладах й факультетах юридичного спрямування, а також при написанні монографій, підручників, посібників (Акт впровадження результатів дисертаційного дослідження у навчальний процес Харківського національного університету внутрішніх від 10 вересня 2015 року).

Апробація результатів дисертації. Результати дисертаційного дослідження пройшли обговорення на засіданнях кафедри кримінального права та кримінології факультету № 1 Харківського національного університету внутрішніх справ. Основні положення й результати дослідження оприлюднювалися та обговорювалися на науково-практичній конференції «Актуальні сучасні проблеми кримінального права та кримінології у світлі реформування кримінальної юстиції» (м. Харків, 12 травня 2012 року) та міжнародній науково-практичній конференції «Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності» (м. Харків, 12 листопада 2014 року).

Публікації. Основні положення й висновки, що сформульовані в дисертаційному дослідженні, опубліковані в 7 наукових працях, у тому числі у 4 наукових статтях в періодичних виданнях України, визнаних фаховими з юридичних наук, у 1 статті, опублікованій у виданні України, яке включено до міжнародної наукометричної бази та 2 тезах наукових доповідей.

Структура дисертації відповідає її меті й задачам та складається з переліку умовних позначень, вступу, трьох розділів, які об’єднують сім підрозділів, висновків, списку використаних джерел та двох додатків. Повний обсяг дисертації становить 213 сторінок, обсяг основного тексту дисертації складає 180 сторінок, список використаних джерел (211 найменувань) розміщений на 24 сторінках, додатки займають 9 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується актуальність теми дисертації, визначається її зв’язок з програмами та планами наукових досліджень, окреслюється рівень наукової розробленості порушеної проблематики, формулюються об’єкт, предмет, мета,

задачі дослідження, описуються його методологічні й методичні засади, основні елементи наукової новизни, відомості щодо їх апробації.

Розділ 1 «Кримінологічна характеристика кіберзлочинності» складається з двох підрозділів.

У *підрозділі 1.1 «Поняття кіберзлочинності та класифікація кіберзлочинів»* сформовано авторське бачення поняття «кіберзлочинність», під якою запропоновано розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку.

Доводиться, що кримінально-правовий обсяг поняття «кіберзлочинність» складають злочини, передбачені ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України, сконцентровані у Розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Відстоюється думка, що предметно-діяльнісна природа злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку визначається посяганнями на віртуалізовану частину (певні складові об'єкту та змісту) суспільних відносин іншого роду – власності, господарських відносин, службової діяльності тощо, – переміщену до кіберпростору, функціонування в якому можливе виключно з використанням вказаних систем і засобів. Відтак, й самі посягання характеризуються, по-перше, специфічною, комбінаційно-цифровою, обстановкою кіберпростору, по-друге, технологічно, системно-технічно та програмно визначеною операційною складовою кримінальної активності, спрямованої на віртуальні компоненти суспільних відносин, спричинення істотної шкоди яким знаходить свій опосередкований прояв у реальній дійсності.

Здійснено класифікацію кіберзлочинів. На підставі 8 критеріїв виділено 61 різновид суспільно небезпечних діянь цієї категорії.

Підрозділ 1.2 «Сучасний стан кіберзлочинності в Україні» містить кримінологічний аналіз показників кіберзлочинності. Аналіз даних офіційної статистичної звітності за останні чотирнадцять років свідчить про тенденцію стабільного та стрімкого зростання рівня кіберзлочинів. Їх середньорічний рівень в інтервалі 2002–2015 рр. склав 205 злочинів. В той же час лише у 2015 році абсолютна кількість зареєстрованих кіберзлочинів сягнула 556, що на 1753,3 % більш ніж у 2002 році та на 33 % більше ніж у 2014. Середньорічний темп приросту протягом 2002–2015 рр. склав 107,5 %. Середньорічний темп зростання за цей же період – 2,075.

Показники динаміки кіберзлочинності в цілому є протилежними відповідним показникам загальної злочинності в країні. Це свідчить: а) про специфічність детермінаційного комплексу кіберзлочинності, в якому протягом 2014–2015 рр. суттєву роль відіграє кібернетична складова зовнішньої агресії проти України; б) про відставання можливостей правоохоронних органів від сучасного рівня технологічного та програмного забезпечення кримінальної активності, в основному

наздоганяючого, а не випереджаючого характеру превентивної та юрисдикційної діяльності поліції.

На підставі аналізу та узагальнення експертних оцінок, матеріалів наукових досліджень встановлено, що рівень латентності кіберзлочинів складає близько 95 %, що дозволяє віднести їх до категорії високолатентних. Серед факторів їх латентності виділено три основні групи: 1) фактори, що обумовлюють природну латентність, в силу яких про вчинений кіберзлочин відомо лише самому винному; 2) фактори, пов'язані з негативною поведінкою жертви (очевидців) злочину та їх незверненням до правоохоронних органів, неповідомленням про факт вчинення злочину; 3) фактори, пов'язані з недоліками роботи правоохоронних органів в частині реагування на звернення та повідомлення про кіберзлочини: а) пов'язані з помилками при прийнятті працівниками правоохоронних органів рішень щодо наявності чи відсутності у вчиненому діянні складу злочину або щодо його кваліфікації; б) пов'язані з приховуванням злочинів від обліку.

Основну частку в структурі кіберзлочинності в Україні складають несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж чи мереж електрозв'язку (56,5 %) та несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (31,5 %). Характерною ознакою структури кіберзлочинності є стабільне зростання частки тяжких злочинів, яка з 2008 року коливається на рівні 45–59 %.

Виявлено, що визначальну роль у відновленні тенденції до зростання рівня кіберзлочинності у 2015 році, після певного спаду у 2014, відіграли злочини, передбачені ст. 361 КК та ст. 361-2 КК України. Загалом у 2015 році відбувся позитивний приріст всіх складових кіберзлочинності, окрім злочинів, передбачених ст. 362 КК України, що є нетиповим з огляду на традиційно вагому частку останніх та їх провідну роль у визначенні характеристик структури кіберзлочинності. Натомість, починаючи з 2013 року темпи приросту цих злочинів суттєво уповільнились, набувши у 2014 та 2015 років негативних значень (- 51,4 % та - 57,7 % відповідно).

У складі групи вчиняється кожен десятий кіберзлочин. З 2006 року фіксується тенденція до зниження частки неповнолітніх з повною їх відсутністю у структурі кіберзлочинності протягом останніх п'яти років.

Встановлено, що розкриваються лише 35–45 % зареєстрованих кіберзлочинів. Засуджується тільки 25 % з числа встановлених осіб, які обвинувачуються у вчиненні злочинів цієї категорії. Таким чином, лише за кожний десятий вчинений кіберзлочин (із зареєстрованих) винні несуть кримінальну відповідальність. Відстоюється думка, що така ситуація є наслідком системних дисфункцій в структурах протидії злочинності, що проявляються у недостатньому науково-методичному, матеріально-технічному, кадровому забезпеченні підрозділів кіберполіції та органів досудового розслідування.

Наголошено на невідповідності судової практики щодо призначення покарань за кіберзлочини характеру й ступеню їх суспільної небезпечності. В переважній більшості засуджені особи звільняються судом від кримінальної відповідальності,

покарання чи його відбування (67 %); серед призначених покарань переважає штраф; в половині випадків призначається більш м'яке покарання, ніж передбачено законом; лише у незначній кількості випадків суд призначає додаткове покарання у виді конфіскації майна (3 %).

Аналіз географії кіберзлочинів в Україні виявив залежність її поширення від фактору урбанізації. Найвища кіберкримінальна активність фіксується за ранжиром в Дніпропетровській області, м. Києві, а також Харківській, Запорізькій та Черкаській областях. Найнижча – в Чернівецькій, Херсонській, Сумській, Кіровоградській областях. Крім того, слід відзначити випадки реєстрації кіберзлочинів на залізниці (Одеська залізниця), що засвідчує поступову експансію кіберзлочинності на більшість сфер життєдіяльності нашого суспільства.

Розділ 2 «Особистість кіберзлочинця та особливості детермінації кіберзлочинності» містить два підрозділи.

У *підрозділі 2.1 «Особистість кіберзлочинця»* здійснено аналіз соціально-демографічних, кримінально-правових та морально-психологічних ознак осіб, винних у вчиненні кіберзлочинів на підставі усереднених даних статистичної звітності Державної судової адміністрації України за 2004–2015 рр. та узагальнень відомостей з матеріалів кримінальних справ й проваджень. У результаті проведеного аналізу встановлено, що в більшості своїй кіберзлочинці – це працездатні, але не працюючі (43,7 %), неодружені (58 %) або одружені, але такі, що з родиною не живуть (16 %), чоловіки (90,8 %), віком 30–50 років (43,1 %), громадяни України (95,5 %), які мають вищу освіту (48,1 %). Розподіл засуджених за вчинення кіберзлочинів за родом їх занять виявив, що першою за поширеністю після працездатних непрацюючих осіб є група службовців, на частку яких припадає 17 % (з них 1,7 % – державні службовці). Другою – робітники (16,1 %) та приватні підприємці (11,4 %). На третьому місці за поширеністю перебувають особи, які навчаються – 7,4 % (6,9 % складають студенти навчальних закладів, 0,5 % – учні шкіл, ліцеїв, коледжів, гімназій). На четвертому – працівники господарських товариств (3,3 %), на п'ятому – пенсіонери (1,1 %).

Питома вага осіб, які на момент вчинення кіберзлочину мали не зняту та непогашену судимість, у структурі засуджених є відносно сталою протягом останніх 5 років та складає 5,8 %. З них 5 % мають одну, 0,8 % – дві судимості. Основну частину цих осіб складають такі, попередня судимість яких пов'язана із вчиненням злочинів проти власності (67 %), злочинів у сфері незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів (27 %), злочинів проти життя та здоров'я особи (3 %), проти громадського порядку та моральності (2 %), інших злочинів – 1 %. В результаті дослідження не виявлено жодного кіберзлочинця, який би вчинив злочини у стані сп'яніння.

Серед мотивів кіберзлочинів переважають корисливі, ігрові, політичні та хуліганські (нігілістичні, самоствердження тощо). Відтак, серед морально-психологічних рис кіберзлочинців превалюють корисливість, авантюризм, правовий та моральний нігілізм, поєднані з детермінованим специфікою кіберпростору комплексом сваволі та ілюзій.

У *підрозділі 2.2* «*Особливості детермінації кіберзлочинності»* відстоюється думка про те, що детермінаційний комплекс кіберзлочинності репрезентований

широким спектром суспільних протиріч політико-правового, соціально-економічного, організаційно-управлінського та культурно-психологічного характеру.

Політико-правові фактори детермінації кіберзлочинності полягають у неузгодженості позицій урядів різних держав з питань інформаційної політики та дотримання прав особи у кіберпросторі; відсутності єдиної державної стратегії України щодо забезпечення кібернетичної безпеки; нестачі політичної волі для належного правового врегулювання інформаційних відносин в частині запобігання інтенсифікованим як внутрішнім, так і зовнішнім, транскордонним кіберзагрозам, в тому числі кримінальним.

Відстоюється думка, що соціально-економічні фактори кіберзлочинності не є для неї специфічними, але, тим не менш, суттєвими. Традиційно криміногенними з тенденцією до загострення лишаються такі з них: розшарування населення за майновою ознакою, падіння рівня життя, безробіття, інфляція. Акцентовано увагу на тому, що окремим, похідним від глобалізаційних процесів, соціально-економічним фактором кіберзлочинності є трансформація господарської діяльності міжнародного рівня з превалюванням її сегменту в кіберпросторі. Нарощування обсягів міжнародних безготівкових розрахунків (в тому числі й з активізацією трудової міграції), інтернет-банкінгу є кореляційними та обумовлюючими чинниками кіберзлочинності.

Організаційно-управлінські фактори кіберзлочинності полягають у недоліках соціального контролю, що виражаються в ігноруванні користувачами всіх рівнів вимог інформаційної безпеки, вадах фінансового та наукового забезпечення її функціонування; дефектах в системі організації і практичного забезпечення технічного захисту комп'ютерних мереж як одного з найуразливіших елементів сучасного технологічно залежного суспільства; низькому рівні підготовленості правоохоронних органів з питань протидії кіберзлочинності, нестачі кваліфікованих кадрів, неналежних матеріально-технічних умовах превентивної діяльності, ефективного науково-методичного супроводження практики виявлення, розкриття та розслідування кіберзлочинів тощо.

Культурно-психологічні фактори обумовлюються соціально значущою активністю у віртуальному середовищі, для певних секторів якого характерним є ціннісно-світоглядний вакуум, знеособлення суспільних відносин та девальвація їх олюдненого значення, деформація нормативних систем координат. Функціонування індивідууму в таких умовах сприяє його соціальній дезорганізації, конфлікту зі складовими реальних сфер життєдіяльності, який вирішується на базі закріплених антисуспільних установок, концентровано виражених у комплексі сваволі та ілюзій.

Розділ 3 «Запобігання кіберзлочинності органами внутрішніх справ та Національною поліцією» складається з трьох підрозділів.

У *підрозділі 3.1 «Правове регулювання запобігання кіберзлочинності органами внутрішніх справ та Національною поліцією»* охарактеризовані правові засади діяльності ОВС та Національної поліції у сфері запобігання кіберзлочинності. Акцентовано увагу на окремих системно-правових недоліках, пов'язаних із незавершеністю процесу реформування правоохоронних органів, прогалинах у правовому регулюванні деяких аспектів кримінально-превентивної практики як Національної поліції, так і ОВС. Наведено додаткові аргументи на користь

необхідності розробки та прийняття Закону України «Про органи внутрішніх справ», в якому має бути передбачено структурно-функціональні елементи ОВС, відповідальні за розробку державної політики та моніторинг діяльності у сфері запобігання кіберзлочинності. З цією метою запропоновано створити на рівні апарату Міністра внутрішніх справ моніторинговий центр протидії злочинності з відповідним сектором у його складі, який відповідатиме за спостереження, оцінку стану кіберзлочинності, контроль реалізації антикримінальних програм.

У *підрозділі 3.2* «*Система заходів запобігання кіберзлочинності органами внутрішніх справ та Національною поліцією*» надано характеристику спеціально-кримінологічних та індивідуальних заходів запобігання кіберзлочинності ОВС і Національною поліцією. Серед пріоритетних напрямів їх удосконалення запропоновано формування та ведення оперативних і профілактичних обліків визначених груп суб'єктів підвищеного кіберкриміногенного ризику, а також посилення контролю за обігом технічних засобів, заборонених або обмежених у цивільному обігу. Акцентовано увагу на необхідності активізації превентивної діяльності щодо виявлення осіб, схильних до вчинення кіберзлочинів, запобігання й припинення їх кримінальної активності. Визначено групу пріоритетного превентивного впливу, яка складається з 18 категорій осіб, штатні посади яких на підприємствах, установах і організаціях обумовлюють високий ризик вчинення кіберзлочинів.

Доводиться необхідність інтенсифікації практики планових та позапланових перевірок підприємств, установ та організацій, основна діяльність яких безпосередньо пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг та забезпечення заходів безпеки на об'єктах, що призначені для передачі інформації. Важливими аспектами удосконалення запобіжної діяльності лишаються: а) впровадження передового досвіду діяльності зарубіжних правоохоронних органів у цій сфері; б) активізація міжнародного співробітництва щодо розкриття, розслідування та запобігання кіберзлочинам; в) формування сучасних комплексних механізмів захисту від кібератак мережевих ресурсів органів державної влади.

Обґрунтовується необхідність розробки та затвердження МВС Стратегії протидії кіберзлочинності як результату діяльності спільної робочої групи МВС та Національної поліції. В її основу повинно бути покладено комплексне опрацювання кримінологічної інформації про стан, тенденції відтворення кіберзлочинності, відповідних кримінологічних прогнозів, а також відповідна концепція кримінально-превентивої діяльності щодо деструкції детермінаційного комплексу кіберзлочинності, науково обґрунтовані стратегічні й тактичні заходи антикримінального впливу, моніторингові механізми забезпечення його якості.

У *підрозділі 3.3 «Взаємодія органів внутрішніх справ та Національної поліції з іншими суб'єктами запобігання кіберзлочинності»* запропоновано напрями здійснення та розвитку взаємодії ОВС й Національної поліції з СБУ, Міністерством освіти і науки, Державною службою спеціального зв'язку та захисту інформації України, Інтернет-провайдерами, приватними ІТ-компаніями, громадськими організаціями з метою підвищення ефективності запобігання кіберзлочинності. Акцентовано увагу на необхідності розширення спектру заходів

міжнародного співробітництва щодо протидії транскордонним проявам кіберзлочинності, зокрема розроблення національних організаційно-правових, технічних і технологічних механізмів приєднання до мережі щоденного цілодобового доступу «24/7 Network» з метою активізації співпраці та надання допомоги при розкритті й розслідуванні кіберзлочинів.

ВИСНОВКИ

Проведене дослідження містить теоретичне узагальнення й нове вирішення наукового завдання, що виявляється у здійсненні комплексної кримінологічної характеристики кіберзлочинності та формуванні науково обґрунтованих пропозицій і рекомендацій, спрямованих на підвищення ефективності запобігання її відтворенню ОВС та Національною поліцією. Основні висновки полягають у такому:

1. Під кіберзлочинністю запропоновано розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку. Доводиться, що прояви кіберзлочинності мають кримінально-правові межі, що визначаються переліком злочинів, ознаки яких закріплені у ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України.

2. Здійснено комплексну класифікацію кіберзлочинів фасетним способом, в результаті чого виділено 61 різновид цих злочинів на підставі 8 критеріїв: особистісних рис злочинця, мотивів злочину, особливостей механізму злочинної, віктимної поведінки, організованості, епізодичності злочинної діяльності, а також залежно від наявності чи відсутності рецидиву злочинів і їх технологічної складової.

3. Охарактеризовано сучасний стан кіберзлочинності в Україні через опис і пояснення її кількісних та якісних показників. Встановлено, що рівень кіберзлочинності у 2015 році склав 556 злочинів і має тенденцію зростання, а саме: середньорічний темп приросту протягом 2002–2015 рр. складає 107,5 %; середньорічний темп зростання за цей же період – 2,075. Показники динаміки кіберзлочинності в цілому є протилежними відповідним показникам загальної злочинності в країні в цілому. Встановлено, що рівень латентності кіберзлочинів складає близько 95 %, що дозволяє їх віднести до категорії високолатентних.

Характерними ознаками показників кіберзлочинності є стабільне зростання частки тяжких злочинів, груповий характер їх вчинення, а також рецидив злочинів, залежність географії поширення від фактору урбанізації. Найвища кіберкримінальна активність фіксується за ранжиром в Дніпропетровській області, м. Києві, а також Харківській, Запорізькій та Черкаській областях. Найнижча – в Чернівецькій, Херсонській, Сумській, Кіровоградській.

4. Надано характеристику особистості кіберзлочинця, визначено її специфічні риси. В більшості своїй – це працездатні, але не працюючі (43,7 %), неодружені (58 %), а також одружені, але такі, що з родиною не живуть (16 %), чоловіки (90,8 %), віком 30–50 років (43,1 %), громадяни України (95,5 %), які мають вищу освіту (48,1 %) і в структурі морально-психологічних якостей яких превалюють

корисливість, правовий нігілізм, авантюризм, поєднані з детермінованим специфікою кіберпростору комплексом сваволі та ілюзій. Мотиви кіберзлочинів є стандартними і принципово не відрізняються від інших видів злочинів: користь, ігрові, політичні, хуліганські мотиви, помста.

5. Досліджено особливості детермінації кіберзлочинності та встановлено, що вони обумовлені роллю кіберпростору як середовища формування особистості злочинця, а також як сукупності обставин, що існують незалежно від особи, яка вчинила злочин (середовища вчинення злочину, яке визначає обстановку його вчинення) та його взаємозв'язком з відповідними факторами реального простору (соціального середовища). Сукупність усіх взаємопов'язаних та взаємодіючих факторів детермінації кіберзлочинності за їх приналежністю до тієї чи іншої групи умовно диференційовано на політико-правові, соціально-економічні, організаційно-управлінські та культурно-психологічні.

6. Охарактеризовано правові засади запобігання кіберзлочинності ОВС і Національною поліцією. Визначено низку міжнародних нормативно-правових актів, а також актів Верховної Ради України, Президента України, Кабінету Міністрів України, відомчих нормативно-правових актів, які складають основу протидії кіберзлочинності в Україні.

Встановлено, що прийняття Закону України «Про національну поліцію» та поява відповідного центрального органу виконавчої влади не потягнуло за собою цілковиту елімінацію кримінально-превентивної функції ОВС, в тому числі й в частині запобігання кіберзлочинності. Відстоюється думка про те, що успішне виконання превентивних задач поліцією можливе за умови належного правового регулювання координуючої та інформаційно-аналітичної діяльності МВС, у зв'язку з чим існує необхідність у прийнятті Закону України «Про органи внутрішніх справ».

7. Визначено та описано систему заходів запобігання кіберзлочинності ОВС і Національною поліцією, вироблено пропозиції щодо її удосконалення. Пріоритетними запобіжними заходами визначено: 1) удосконалення системи оперативного супроводження підприємств, установ та організацій, основна діяльність яких пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг та забезпечення заходів безпеки на об'єктах, що призначені для передачі інформації; 2) запровадження та ведення спеціалізованих профілактичних обліків; 3) розроблення, затвердження та реалізація МВС Стратегії протидії кіберзлочинності; 4) формування сучасних комплексних механізмів захисту від кібератак мережевих ресурсів органів державної влади та інше.

8. Досліджено наукові засади та прикладні аспекти взаємодії органів внутрішніх справ і Національної поліції з іншими суб'єктами запобігання кіберзлочинності та запропоновано на цій підставі шляхи її оптимізації, а саме: удосконалення взаємодії підрозділів Національної поліції з СБУ, Міністерством освіти і науки України, Державною службою спеціального зв'язку та захисту інформації України; підтримання та розвиток співробітництва з науковими установами; підтримання та розвиток взаємодії із провайдерами Інтернет-послуг; удосконалення взаємодії з підприємствами, установами та організаціями, діяльність яких пов'язана з розробкою комп'ютерної техніки та програмного забезпечення;

розроблення національних організаційно-правових, технічних і технологічних механізмів приєднання до мережі щоденного цілодобового доступу «24/7 Network» з метою активізації співпраці та надання допомоги при розкритті й розслідуванні кіберзлочинів тощо.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Кравцова М. О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії / М. О. Кравцова // Юридичний науковий електронний журнал. – 2014. – № 5 . – С. 110–113 [Електронний ресурс]. – Режим доступу : http://lsej.org.ua/5_2014/5_2014.pdf.

2. Кравцова М. О. Проблеми правового регулювання запобігання кіберзлочинності органами внутрішніх справ / М. О. Кравцова // Європейські перспективи. – 2014. – № 10. – С. 118–124.

3. Кравцова М. О. Система заходів запобігання кіберзлочинності правоохоронними органами / М. О. Кравцова // Митна справа. – 2014. – Спеціальний випуск. – С. 164–169.

4. Кравцова М. О. Сучасний кіберзлочинець: кримінологічна характеристика особистості / М. О. Кравцова // Митна справа. – 2015. – № 4 (100). – Ч. 2. – С. 46–53.

5. Кравцова М. А. Понятие киберпреступности и ее признаки / М. А. Кравцова // Часопис Київського університету права. – 2015. – № 2. – С. 48–54.

6. Кравцова М. О. Сучасне кримінологічне поняття кіберзлочинності / М. О. Кравцова // Актуальні сучасні проблеми кримінального права та кримінології у світлі реформування кримінальної юстиції : Матер. Всеукраїнської наук.-практ. конф. (м. Харків, 12 травня 2012 року) / МВС України ; Харківський національний університет внутрішніх справ ; Кримінологічна асоціація України. – Т. 1. – Х. : Золота миля, 2012. – С. 248–250.

7. Кравцова М. О. Мотивація кіберзлочинів: дані емпіричного дослідження / М. О. Кравцова // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : Матер. міжнар. наук.-практ. конф. (м. Харків, 12 листопада 2014 р.). – Х. : Права людини, 2014. – С. 89–92.

АНОТАЦІЇ

Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ. – *На правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право. – Харківський національний університет внутрішніх справ, Харків, 2016.

Дисертацію присвячено комплексній кримінологічній характеристиці кіберзлочинності та проблемам запобігання їй органами внутрішніх справ і Національною поліцією України.

У роботі визначено поняття кіберзлочинності та надано класифікацію кіберзлочинів. Охарактеризовано сучасний стан кіберзлочинності в Україні:

встановлено її рівень, динаміку, величину та фактори латентності, структуру, географію. Надано характеристику особистості кіберзлочинця. Виявлено, описано та проаналізовано соціально-демографічні, кримінально-правові та морально-психологічні риси осіб, засуджених за вчинення кіберзлочинів. Встановлено та проаналізовано основні політико-правові, соціально-економічні, організаційно-управлінські та культурно-психологічні фактори кіберзлочинності.

Досліджено стан та запропоновано шляхи удосконалення правового регулювання діяльності органів внутрішніх справ і Національної поліції щодо запобігання кіберзлочинності. Вироблено рекомендації, спрямовані на підвищення ефективності кримінально-превентивної практики вказаних органів, а також їх взаємодії з іншими суб'єктами в частині запобігання кіберзлочинності.

Ключові слова: кіберзлочинність, стан, особистість злочинця, детермінація, запобігання, органи внутрішніх справ, поліція, взаємодія.

Кравцова М. А. Киберпреступность: криминологическая характеристика и предупреждение органами внутренних дел. – *На правах рукописи*.

Диссертация на соискание ученой степени кандидата юридических наук по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. – Харьковский национальный университет внутренних дел, Харьков, 2016.

Диссертация посвящена комплексной криминологической характеристике и предупреждению органами внутренних дел и Национальной полицией Украины киберпреступности.

В работе определено понятие киберпреступности, под которой предложено понимать социально-правовой феномен, проявляющийся в запрещенной законом об уголовной ответственности предметной деятельности (криминальной активности) части населения с использованием электронно-вычислительных машин (компьютеров), телекоммуникационных систем, компьютерных сетей и сетей электросвязи.

Осуществлена комплексная классификация киберпреступлений фасетным способом, в результате чего выделен 61 их вид на основании 8 критериев: личностных признаков преступника, мотивов преступления, особенностей механизма преступного и виктимного поведения, организованности, эпизодичности преступной деятельности, а также в зависимости от наличия или отсутствия рецидива преступлений и их технологической составляющей. Охарактеризовано современное состояние киберпреступности в Украине, в результате чего установлены её высокий уровень, неблагоприятная динамика с тенденцией к положительному приросту, высокая латентность, осложненная групповыми формами криминальной активности, а также рецидивом преступлений структура, зависящая от фактора урбанизации география. Дана характеристика личности киберпреступника. Выявлены, описаны и проанализированы социально-демографические, уголовно-правовые и морально-психологические черты лиц, осужденных за совершение киберпреступлений. Установлены и проанализированы основные политико-правовые, социально-экономические, организационно-управленческие и культурно-психологические факторы киберпреступности.

Исследовано состояние и разработаны пути совершенствования правового регулирования деятельности органов внутренних дел и Национальной полиции по предупреждению киберпреступности. Предложена система предупредительных мер, осуществляемых ОВД и Национальной полицией, которая включает превентивную деятельность на специально-криминологическом и индивидуальном уровнях, которая предполагает концептуально целостное, согласованное и управляемое воздействие на детерминационный комплекс киберпреступности с учетом специфики внутригосударственных общественных противоречий, а также потребностей в реагировании на изменчивые факторы развития компьютерных технологий, проявления внешней агрессии по отношению к Украине, которая разворачивается в том числе и в киберпространстве. Обоснована необходимость формирования и ведения оперативных, профилактических учетов субъектов повышенного киберкриминогенного риска, а также усиления контроля за оборотом технических средств, запрещенных или ограниченных в гражданском обороте, присоединения к международным программам и технологическим системам противодействия киберпреступности.

Ключевые слова: киберпреступность, состояние, личность преступника, детерминация, предупреждение, органы внутренних дел, полиция, взаимодействие.

Kravtsova M. O. Cybercrime: Criminological Characteristic and Prevention by Organs of Internal Affairs. – *Published as manuscript.*

Thesis for a Candidate Degree in Law, Speciality 12.00.08. – Criminal Law and Criminology; Criminal Executive Law. – Kharkiv National University of Internal Affairs, Kharkiv, 2016.

Dissertation is devoted to a complex criminological characteristic and prevention of cybercrime by organs of internal affairs and National police .

The work defines the notion of cybercrime and provides classification of cybercrimes. It characterizes present state of cybercrime in Ukraine: defines its rate, dynamics, magnitude and factors of latency, structure, geography.

The dissertation provides characteristic of peculiarities of a cybercriminal. It defines, describes and analyses social-demographic, criminal and legal, moral and psychological characteristics of persons, convicted for committing cybercrimes. The work defines and analyses political-legal, social-economical, organizational-administrative and cultural-psychological factors of cybercrime.

The dissertation examines the state of legal regulation of activities of organs of internal affairs and National police in the sphere of cybercrime prevention and proposes way of its enhancement. It works out recommendations for enhancement efficiency of crime prevention practice of the organs mentioned and their cooperation with other subjects in cybercrime prevention.

Key words: cybercrime, state, peculiarities of a criminal, determination, prevention, organs of internal affairs, police, cooperation.

Підписано до друку 18.02.2016 р. Папір офсетний. Друк офсетний.
Формат 60х84/16. Умов. друк. арк. 0,9. Обл.-вид. арк. 0,9.
Наклад 100 прим.

Видавець і виготовлювач −
Харківський національний університет внутрішніх справ,
пр-т Льва Ландау, 27, м. Харків, 61080.
Свідоцтво суб'єкта видавничої справи ДК № 3087 від 22.01.2008.

Друкарня Харківського національного університету внутрішніх справ
61080, м. Харків, пр-т Льва Ландау, 27.