УДК 343.98

КРИТЕРІЇ РОЗМЕЖУВАННЯ ШКІДЛИВИХ ТЕХНІЧНИХ ЗАСОБІВ ТА ТЕХНІЧНИХ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Олександр КУРМАН,
кандидат юридичних наук, доцент, доцент кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого

У статті аналізуються критерії віднесення технічних засобів, що можуть використовуватися при вчиненні злочинів у сфері інформаційних технологій, до різних груп, визначається різниця між шкідливими технічними засобами та технічними засобами негласного отримання інформації. На підставі аналізу наводяться схожі властивості та характеристики й визначається різниця між ними, яка полягає в тому, що шкідливі технічні засоби виготовляються не уповноваженими суб'єктами, заздалегідь не призначаються для використання у спеціальні характерні способи в правоохоронній діяльності та результатами їх застосування є настання негативних наслідків у вигляді витоку, втрати, блокування, підробки інформації, спотворення процесу її оброблення або порушення порядку маршрутизації.

Ключові слова: *шкідливі технічні засоби, засоби негласного отримання інформації, інформаційні технології, способи вчинення, методика розслідування.*

DETERMINATION CRITERIA FOR HARMFUL TECHNICAL MEANS AND MEANS OF SECRETLY OBTAINING Of THE INFORMATION

Oleksandr KURMAN,
Candidate of Law Sciences, Associate Professor, Associate Professor at the Department of Criminalistics
of Yaroslav Mudryi National Law University

The article analyzes the criteria for attributing technical means that can be used in committing crimes in the field of information technology to different groups, and determines the difference between harmful technical means and technical means of secretly obtaining information. Similar properties and characteristics are given and it is determined that the difference between them is that the harmful technical means are manufactured by unauthorized subjects, are not intended in advance for use in special characteristic ways in law enforcement activity and the results of their application are negative consequences in the form of leakage, loss, blocking, falsification of the information, distortion of the process of its processing or disruption of routing.

Keywords: *harmful technical means, means of secretly obtaining information, information technology, methods of crime, methodology of the investigation.*

CRITERII PENTRU DELIMITAREA MIJLOACELOR TEHNICE DĂUNĂTOARE ŞI A MIJLOACELOR TEHNICE DE PRELUARE SILENȚIOASĂ A INFORMAȚIILOR

Articolul analizează criteriile de atribuire a mijloacelor tehnice care pot fi utilizate în comiterea infracțiunilor din sfera tehnologiei informaționale diferitelor grupuri, determină diferența dintre mijloacele tehnice dăunătoare și mijloacele tehnice de achiziție a informațiilor silențioase. Pe baza analizei, se dau proprietăți și caracteristici similare și se stabilește diferența dintre acestea, ceea ce înseamnă că mijloacele tehnice dăunătoare sunt fabricate de către subiecți neautorizați, nu sunt destinate în avans pentru utilizare în moduri caracteristice speciale în activitatea de aplicare a legii, iar rezultatele aplicării lor sunt consecințe negative sub formă de scurgere, pierdere, blocare, falsificare a informațiilor, denaturarea procesului de prelucrare a acesteia sau întreruperea rutării.

Cuvinte-cheie: *mijloace tehnice dăunătoare, mijloace de obținere silențioasă a informațiilor, tehnologii informaționale, metode de comitere, tehnică de investigare.*

Постановка проблеми. Сьогодні світ вже не може існувати та розвиватися без цифрових технологій. Практично кожен мешканець України тією або іншою мірою користується їх можливостями. Насамперед, це мобільний зв'язок та інтернет, ефірне, супутникове та IPTV телебачення, електронна комерція та безготівкові розрахунки, створення центрів надання адміністративних послуг, де громадяни можуть отримати різноманітні документи або послуги, замовивши їх через мережу інтернет тощо. Міністерство цифрової трансформації України запустило новий проект «Цифрова держава», в рамках якого впровадило новий мобільний додаток «Дія» та національну онлайн-платформу цифрової освіти. На черзі реалізація наступних проектів: електронне

урядування, електронна демократія, електронний суд та інші. Практично майже всі підприємства, установи, організації перейшли (чи переходять) на систему ведення електронного бухгалтерського обліку. Реєстри та бази даних державних установ також набули трансформації в електронну форму.

На жаль, можливості цифрових технологій використовуються не тільки з метою створення нових благ. Злочинний світ також повною мірою взяв на озброєння наукові та технічні досягнення в цій сфері. Серед привабливих напрямів використання сучасних цифрових технологій можна виділити такі: промисловий та комерційний шпіонаж, системи державного управління, облікові дані користувачів, фейкові новини, конфіденційність особистого життя (в тому числі, в перспективі, перехоплення керування над системами «smart car» та «smart house»). Також не можна не враховувати таку серйозну загрозу, як кібертероризм.

Актуальність теми дослідження. Вчинення зазначених вище протиправних посягань, окрім високої теоретичної підготовки, потребує використання злочинцями сучасних технічних засобів. На сьогодні на озброєнні кіберзлочинців знаходиться дуже широкий спектр різноманітного технічного устаткування, починаючи від побутових комп'ютерів, гаджетів і саморобних пристроїв до складних програмно-технічних комплексів, виготовлених на замовлення. Саме тому виникає гостра необхідність у забезпеченні надійного криміналістичного забезпечення захисту інформації від несанкціонованого втручання та розроблення нових методів у розслідуванні злочинів у сфері інформаційних технологій.

Стан дослідження. Обов'язковим етапом розроблення чи вдосконалення будь-якої методики розслідування злочинів є дослідження елементів криміналістичної характеристики. Зазначеній криміналістичній категорії у різні часи було присвячено чимало наукових праць. Так, даній проблематиці присвятили свої роботи такі вчені, як: В.О. Голубєв, В.А. Журавель, А. Д. Марушев, О.І. Мотлях, Л.П. Паламарчук, В.Г. Танасевич, та ін.[1; 2; 3, с. 227-230; 4; 5, с. 150-153; 6, с. 99-100]. Однак з урахуванням специфіки сьогодення та постійного розвитку сучасних технологій дослідження видів технічних засобів, що використовуються для вчинення злочинних посягань на інформацію, яка зберігається або обробляється в електронних системах, комп'ютерних мережах, їх характеристик, способів використання, є вкрай актуальними та потребують постійного оновлення.

Метою і завданням статті є аналіз існуючих критеріїв віднесення технічних засобів, що використовуються під час вчинення злочинів у сфері інформаційних технологій, до різних класифікаційних груп, а також визначення різниці між шкідливими технічними засобами та технічними засобами негласного отримання інформації під час вчинення несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Виклад основного матеріалу. Кримінальне законодавство України містить низку статей, які прямо або опосередковано стосуються незаконного виготовлення, використання, збуту, розповсюдження технічних засобів, що використовуються для несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – ст. 359 КК (незаконне придбання, збут або використання спеціальних технічних засобів отримання інформації; ст. 361 КК (несанкціоноване втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ст. 361-1 КК (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут),

Як бачимо, кримінальний закон виділяє два види технічних засобів, які потенційно можуть бути використані (використовуються) для вчинення злочинів у сфері інформаційних технологій. По-перше, це спеціальні технічні засоби отримання інформації, а по-друге – шкідливі технічні засоби. На жаль, визначення шкідливих технічних засобів законодавець не надає. Виходячи з аналізу диспозиції ст. ст. 361, 361-1 КК України можна виділити низку ознак, за якими технічний засіб стає предметом злочину. Такими ознаками є: 1) шкідливість, 2) призначеність для несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку.

Тлумачний словник визначає «шкідливий» як такий, що завдає шкоди, збитків кому-, чому-небудь чи в чомусь; негативно впливає на когось, щось [7, с. 474]. Враховуючи специфічність суспільних відносин, на які посягає злочин, особливості механізму злочинних дій, слідову картину, можна визначити, що така шкода, негативний вплив може виявлятися у витоку, втраті, підробці, блокуванні інформації, спотворенні процесу обробки інформації або у порушенні встановленого порядку її маршрутизації.

Пояснення суті деяких видів наслідків прямо

наведено у Законі або логічно витікає із визначення термінів. Виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї. Блокування інформації – дії, внаслідок яких унеможливлюється доступ до інформації в системі [8]. Втрата інформації – ситуація, коли інформація, яка раніше існувала в системі, перестає існувати для фізичних або юридичних осіб, які мають право власності на неї, в повному чи обмеженому обсязі. Підробка інформації означає несанкціоновану власником чи уповноваженою ним особою зміну інформації. Спотворення процесу обробки інформації – зміна методики чи процесу обробки інформації комп'ютером чи АС, внаслідок якої обробка інформації не дає результатів взагалі, дає неправильні результати або ж дає лише частину тих результатів, які можна було отримати до цієї зміни. Порушенням встановленого порядку маршрутизації інформації слід вважати зміну режиму роботи мережі електрозв'язку, внаслідок якої певна інформація, що передається у цій мережі, потрапляє чи може потрапити у розпорядження особи, яка за умов нормальної роботи мережі не повинна була отримати цю інформацію [9].

Характеризуючи ознаку «призначеність для несанкціонованого втручання», необхідно виходити із наступного. У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» наводиться дефініція такої категорії як «несанкціоновані дії щодо інформації в системі», до яких відносяться такі, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства. Згідно зі ст. 1 зазначеного Закону доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі. Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації. Обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. Виходячі з аналізу наведених категорій, можна зробити висновок, що несанкціоноване втручання в роботу – це порушення користувачем умов та правил отримання і обробки інформації. Такі умови та правила отримання і обробки інформації встановлюються володільцем інформації. [10, с. 246].

Враховуючи те, що одним із наслідків застосування шкідливих технічних засобів є виток інформації, внаслідок якого вона стає відомою іншим особам, в цьому випадку вбачається деяка подібність з процесуальними діями, що проводяться під час розслідування кримінальних правопорушень. Під час їх проведення також використовуються технічні засоби, які дозволяють отримати інформацію без згоди її володільця або з недотриманням правил та умов, встановлених такою особою, тобто мають таку ознаку як негласність отримання інформації. Значення терміну «негласне отримання інформації» розкривається у Постанові КМУ від 22.09.2016 року № 669, якою затверджено «Критерії належності спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації», і визначається як «заходи, що здійснюються для отримання інформації з обмеженим доступом без відома і згоди суб'єкта цієї інформації» [11].

Законодавство України дозволяє отримувати інформацію з телекомунікаційних мереж за допомогою технічних засобів без згоди володільця та в порушення встановлених ним правил. Так, Законами України «Про телекомунікації» [12] та «Про захист інформації в інформаційно-телекомунікаційних системах» [8] у ст. 9. та ст. 4 відповідно закріплено, що зняття інформації з телекомунікаційних мереж, доступ до неї в системі може здійснюватися без дозволу володільця в порядку, встановленому законом. КПК України визначає ситуації, коли умови та правила отримання інформації можуть бути порушені на законних підставах. Зокрема, під час проведення обшуку (ст. 234 КПК) і негласних слідчих (розшукових) дій - зняття інформації з транспортних телекомунікаційних систем (ст. 263 КПК) та зняття інформації з електронних інформаційних систем (ст. 264 КПК). Для такого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, як відомо, необхідна ухвала слідчого судді.

До технічних засобів, що можуть на законних підставах використовуватися під час зазначених слідчих дій для отримання, перетворення, фіксації інформації та досягнення інших цілей, їх виробництва, також пред'являються певні вимоги. У відповідності до ст. 7 Закону України «Про ліцензування видів господарської діяльності» [13] діяльність, пов'язана з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації підлягає ліцензуванню. Органом ліцензування

щодо такої діяльності згідно Постанови КМУ від 05 серпня 2015 року № 609 «Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України» [14] визначено Службу безпеки України. Зазначені технічні засоби повинні виготовлятися, реалізовуватися в порядку, встановленому Постановою КМУ від 27.10.2001 року № 1450 «Про затвердження Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації»[15]. Якщо вказані технічні засоби є імпортного виробництва та мають ознаки товарів подвійного призначення, то їх постачання на територію України повинно відбуватися згідно правил, встановлених Законом України від 20.02.2003 року «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» [16] та Постановою КМУ від 28.01.2004 № 86 «Про порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання» [17].

Необхідно розрізняти шкідливі технічні засоби, що використовуються для несанкціонованого втручання в роботу зазначених вище об'єктів, виготовляються для цих цілей або збуваються, та технічні засоби негласного отримання інформації, які використовуються на законних підставах для втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

При вирішенні питання щодо розмежування шкідливих технічних засобів та спеціальних технічних засобів негласного отримання інформації необхідно виходити з наявної сукупності двох критеріїв, встановлених законодавством України:

- призначеність засобів для застосування у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності;
- придатність засобів для негласного отримання інформації.

Відповідно до згадуваної вище Постанови КМУ від 22.09.2016 року № 669 наявність окремих ознак (мініатюрні розміри, багатофункціональність, можливість негласного використання та отримання інформації) не може розглядатися як приналежність до спеціальних технічних засобів негласного отримання інформації. У разі, якщо технічний вироб в силу, наприклад, багатофункціональності, може бути використаний для негласного отримання інформації, але виробником спеціально не розроблявся та не виготовлявся для застосування у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності, то він не відноситься до таких спеціальних технічних засобів. Заслуговує на схвалення той факт, що на законодавчому рівні визначено хоча б загальні критерії віднесення виробів до спеціальних, однак викликає питання, що таке «скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності»? Законодавство України не містить визначення цієї категорії, не наводить критерії, ознаки способу, характерного для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності.

На сьогодні це питання вирішується шляхом проведення судової експертизи спеціальних технічних засобів негласного отримання інформації в Центрі судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України та його зональних підрозділах в областях. Також типовими експертизами при розслідуванні злочинів у сфері інформаційних технологій є експертиза комп'ютерної техніки і програмних продуктів (наприклад, встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення, якщо шкідливі технічні засоби програмувалися чи перепрограмувалися для вчинення злочину), експертиза телекомунікаційних систем та засобів (для визначення характеристик та параметрів шкідливих технічних систем та засобів; встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій тощо); електротехнічна експертиза (для встановлення способу підключення та наслідків цього) та ін.

Створення шкідливих технічних засобів являє собою результат діяльності щодо розроблення таких засобів у вигляді нового технічного засобу або вдосконалення (модифікація) вже існуючого. Причому, виготовлення може мати форму налагодження пристрою або його програмування.

Розповсюдження шкідливих технічних засобів аналогічне простому розповсюдженню матеріальних предметів. Однак і це діяння має певну специфіку. Крім простого передавання таких засобів, можливим є їх установлення в електронно-обчислювальні машини, системи або комп'ютерні мережі, які продаються або передаються на іншій основі, наприклад, здаються в оренду. Розповсюдження шкідливих технічних засобів – це оплатне або безоплатне передавання технічного засобу,

а також його встановлення в ЕОМ, системи або комп'ютерні мережі. Збут шкідливих технічних засобів відрізняється від розповсюдження тим, що він пов'язаний з відчуженням предмета. Під збутом шкідливих технічних засобів слід розуміти їх оплатне або безоплатне відчуження [18].

Можливості шкідливих технічних засобів побудовані на тому, що практично будь-який прилад, що використовується для збирання, фіксації, обробки, передачі інформації, можна використати як джерело отримання інформації. Це пов'язано з тим, що всі вони випромінюють під час своєї роботи у простір різні види електромагнітної енергії.

Аналіз різноманітних випромінювачів чи перетворювачів свідчить, що:

- генерувати небезпечний сигнал здатна будь-яка електронна та радіоапаратура, а також окремі елементи чи вузли техніки;

- з кожного генерованого небезпечного сигналу можна, за певних обставин, сформувати канал витоку інформації;

- будь-яка електронна система, що складається з комплексу вузлів та елементів, налічує сукупність джерел небезпечного сигналу, які за певних умов можуть перетворитися на канали для витоку інформації [19].

Залежно від призначення шкідливі технічні засоби можуть бути поділені на ті, що використовуються для отримання інформації з: 1) телекомунікаційних мереж; 2) електронних інформаційних систем; 3) конкретного електронного-обчислюваного пристрою; а також для: 4) відеоконтролю та спостереження за конкретним місцем чи устаткуванням; 5) подолання криптографічного захисту. Технічні засоби можуть бути закамуфльовані під побутові та інші речі.

За принципом фізичної дії їх можна класифікувати на:

1) Акустичні. Використовують механічний вплив звукових хвиль на радіоелектронну апаратуру.

2) Електричні - отримують інформацію за рахунок змін величини та характеру струму і напруги в мережах електрозв'язку.

3) Електромагнітні - використовують випромінювання електромагнітних хвиль при роботі обладнання.

4) Оптичні - отримують інформацію через розшифровування електромагнітних сигналів у видимому діапазоні світла та невидимому (інфрачервоному, ультрафіолетовому тощо).

Висновок. У сучасному світі злочинці для отримання важливої електронної інформації використовують різноманітні технічні засоби. Ці засоби можуть бути спеціально виготовлені уповноваженими суб'єктами господарської діяльності у відповідності до технічних завдань для використання в оперативно-розшуковій, контррозвідувальній або розвідувальній діяльності, а можуть створюватися злочинцями, які не мають для цього законних підстав та дозволів. Крім того, для досягнення злочинних намірів можуть перероблюватися прилади і устаткування побутового та промислового призначення. Технічні засоби першої та другої групи поділяються на різні види та підвиди, залежно від способу застосування та призначення, базуються на одних принципах роботи та можуть мати схожі характеристики та можливості. Різниця між ними полягає в тому, що шкідливі технічні засоби виготовляються не уповноваженими суб'єктами, заздалегідь не призначалися для використання у спеціальні характерні способи в правоохоронній діяльності та результатами їх застосування є настання негативних наслідків у вигляді витоку, втрати, блокування, підробки інформації, спотворення процесу її оброблення або порушення порядку маршрутизації.

Список використаної літератури

1. Голубєв В. О. Розслідування комп'ютерних злочинів: моногр. Запоріжжя: Гуманіт. ун-т «ЗІДМУ», 2003. 296 с.

2. Журавель В. А. Криміналістичні методики: сучасні наукові концепції: моногр. Х.: Апостіль, 2012. 304 с.

3. Марушев А. Д. Особливості визначення елементів криміналістичної характеристики в процесі розслідування злочинів, пов'язаних з кримінальним банкрутством. *Юридичний науковий електронний журнал* [Електронне наукове видання]. Запоріжжя: ЗНУ, 2016. № 6. С. 227 – 230. URL: http://www.lsej.org.ua/

4. Мотлях О. І. Методика розслідування комп'ютерних злочинів: моногр. К. : Освіта України, 2010. 296 с.

5. Паламарчук Л. П. Криміналістична характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. *Підприємництво, господарство і право*. 2004. №8. С. 150–153.

6. Танасевич В. Г. Криминалистическая характеристика преступлений . *Вопросы борьбы с преступностью*. М., 1976. Вып. 25. С. 99-100.

7. Словник української мови: в 11 томах. АН УРСР. Інститут мовознавства; за ред. І. К. Білодіда. К.: Наукова думка, Том 11. 1980. Стор. 474.

8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від

05.07.1994 року № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

9. Мельник М. І., Хавронюк М. І. Науково-практичний коментар кримінального кодексу України, 2010 URL: http://yport.inf.ua/stattya-361-nesanktsionovane-vtruchannya.html

10. Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство.*2017. № 4. С. 245-249.

11. Критерії належності спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації: Постанова КМУ від 22.09.2016 року № 669. URL: https://zakon.rada.gov.ua/laws/show/669-2016-%D0%BF#n158

12. Про телекомунікації: Закон України від 18.11.2003 року. № 1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15

13. Про ліцензування видів господарської діяльності: Закон України від 02.03.2015 року № 222-VIII. URL: https://zakon.rada.gov.ua/laws/show/222-19

14. Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України: Постанова КМУ від 05 серпня 2015 року № 609. URL: https://zakon.rada.gov.ua/laws/show/609-2015-%D0%BF

15. Про затвердження Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації: Постанова КМУ від 27.10.2001 року № 1450. URL: https://zakon.rada.gov.ua/laws/show/1450-2001-%D0%BF

16. Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання: Закон України від 20.02.2003 року № 549-IV. URL: https://zakon.rada.gov.ua/laws/show/549-15

17. Про порядок здійснення державного контролю за міжнародними передачами товарів подвійного використання: Постанова КМУ від 28.01.2004 року № 86. URL: https://zakon.rada.gov.ua/laws/show/86-2004-%D0%BF#n234

18. Карчевський М. В. Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (тези лекцій). URL: https://it-crime.at.ua/index/shkidlivi_programni_ta_tekhnichni_zasobi/0-34

19. Відоменко О. І. Використання технічних засобів як складова системи економічної безпеки підприємства. *Ефективна економіка* № 7. 2017. URL: http://www.economy.nayka.com.ua/?op=1&z=5684

ІНФОРМАЦІЯ ПРО АВТОРА
КУРМАН Олександр Васильович,
кандидат юридичних наук, доцент, доцент кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого;

INFORMATION ABOUT THE AUTHOR
KURMAN Oleksandr Vasylovych,
Candidate of Law Sciences, Associate Professor, Associate Professor at the Department of Criminalistics of Yaroslav Mudryi National Law University;
reksik9@gmail.com