УДК 343.985

Г. І. Резнікова, аспірант лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків

ОБСТАНОВКА РОЗГОЛОШЕННЯ ПРОФЕСІЙНИХ ТАЄМНИЦЬ ЯК ЕЛЕМЕНТ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ЗЛОЧИНІВ

У статті аналізуються особливості обстановки розголошення професійних таємниць. Зосереджується увага на окремих недоліках, що сприяють розголошенню професійних таємниць. Досліджується час та місце вчинення злочинів щодо розголошення професійних таємниць.

Ключові слова: *професійна таємниця,обстановка вчинення злочину, час вчинення злочину, місце вчинення злочину.*

Вирішення завдання з розбудови криміналістичної характеристики злочинів щодо розголошення професійних таємниць потребує змістовного аналізу її окремих структурних елементів, зокрема, обстановки вчинення злочину. Дослідження обстановки розголошення професійних таємниць дозволяє проаналізувати умови, що сприяють вчиненню вказаної категорії злочинів, та, відповідно, надати методично обґрунтовані рекомендації з їх розкриття і розслідування. Хоча дотепер ученими-криміналістами не було приділено значної уваги вивченню проблем, що виникають у процесі розслідування розголошень професійних таємниць, статистика зареєстрованих правопорушень в Україні за січень – грудень 2013 р.[1]

[1] Статистика кримінальних правопорушень, пов'язаних із розголошенням професійних таємниць, за січень – грудень 2013 р. свідчить, що зареєстровано таку кількість правопорушень: 1) розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132 КК України) – 2; 2) незаконне розголошення лікарської таємниці (ст. 145 КК України) – 4; 3) порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК України) – 18; 4) розголошення таємниці

свідчить про актуальність цього питання. Сьогодні лише незначна кількість, а саме не більше 1–5% випадків від реально існуючих витоків інформації стають надбанням громадськості, зокрема, завдяки висвітленню цих фактів у ЗМІ[1]. Дослідження названої категорії злочинів потребує вивчення обстановки їх вчинення, а також ретельного аналізу тих умов та обставин, що перешкоджають або, навпаки, сприяють реалізації злочинної мети. Отже, метою статті є виявлення та аналіз криміналістично значущих ознак «обстановки вчинення злочину».

Злочин вчиняється у певних умовах дійсності – у зовнішньому середовищі[2], яке у криміналістиці отримало назву «обстановка вчинення злочину». І. М. Якімов писав, що проникнення в обстановку та обставини злочину веде до виразного розуміння скоєного, до осягнення внутрішнього зв'язку між діями, що вчинені злочинною волею, та їх відображенням ззовні[3]. Проте й дотепер серед учених-криміналістів немає єдності з приводу визначення сутності поняття «обстановка вчинення злочину». М. П. Яблоков зазначає, що всі наявні у криміналістиці визначення обстановки вчинення злочину трактують її або занадто широко, або ж, навпа-

усиновлення (удочеріння) (ст. 168 КК України) – 9; 5) порушення недоторканності приватного життя (ст. 182 КК України) – 128; 6) умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму (ст. 209[1] КК України) – 3; 7) незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК України) – 17; 8) розголошення комерційної або банківської таємниці (ст. 232 КК України) – 12; 9) незаконне використання інсайдерської інформації (ст. 232[1] КК України) – 0; 10) розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381 КК України) – 1; 11) розголошення даних досудового слідства або дізнання (ст. 387 КК України) – 14 (див.: Єдиний звіт про кримінальні правопорушення. – Форма № 1 (місячна) : затв. наказом ГПУ від 23 жовт. 2012 р. № 100 за погодженням з Держстатом України [Електронний ресурс]. – Режим доступу: http://www.gp.gov.ua/ua/stst2011.html?dir_id = 110381&libid= 100820&c=edit&_c=fo. – Заголовок з екрана).

[1] Исследование утечек информации и конфиденциальных данных из компаний и госучреждений России в 2012 г. [Электронный ресурс] : отчет об уровне защиты конфиденц. данных, 2013. – С. 16. – Режим доступа: http://www.infowatch.ru/node/3013?sid=5358. – Загл. с экрана.

[2] Ермолович В. Ф. Криминалистическая характеристика преступлений / В. Ф. Ермолович. – Минск : Амалфея, 2001. – С. 166.

[3] Якимов И. Н. Криминалистика. Уголовная тактика / И. Н. Якимов. – Изд. 2-е, перераб. и доп. – М. : НКВД РСФСР, 1929. – С. 75.

ки, занадто вузько[1]. Так, широкий підхід підтримує В. О. Образцов, який відносить до обстановки вчинення злочину територіальну, кліматичну, демографічну та іншу специфіку регіону, в якому вчинено злочин, а також обставини, що характеризують безпосереднє місце, час, умови та інші особливості вказаної життєвої ситуації[2]. Таким чином, досліджуючи проблему визначення змісту поняття обстановки вчинення злочину, можливо віднайти різні позиції криміналістів – від вельми широких до вузьких трактувань цього поняття, лише як змісту матеріальної (речової) обстановки місця вчинення злочину.

Обстановка вчинення злочину є системою різного роду взаємодіючих між собою об'єктів, явищ та процесів, що характеризують умови місця та часу, речові, природно-кліматичні, виробничо-побутові та інші умови оточуючого середовища, особливості поведінки непрямих учасників протиправної події, психологічні зв'язки між ними та інші обставини об'єктивної дійсності, що склалися на момент учинення злочину, які впливають на спосіб його вчинення та механізм, що виявляється в різних слідах, які дозволяють зробити висновок про особливості цієї системи та зміст злочину[3]. Обстановка вчинення злочину включає інформацію, яка характеризує як зовнішній бік злочину (матеріальне середовище), так і внутрішню своєрідність умов та обставин, що сприяли вчиненню кримінально караного діяння. М. П. Яблоков зазначає, що більша частина структурних елементів обстановки вчинення злочину характеризує зовнішнє середовище, а менша – особливості (своєрідність) поведінки непрямих учасників злочину, особливості психологічних зв'язків між усіма учасниками розслідуваної події та інші фактори об'єктивної дійсності[4].

[1] Яблоков Н. П. Обстановка совершения преступления как элемент его криминалистической характеристики / Н. П. Яблоков // Криминалистическая характеристика преступлений : сб. науч. тр. – М. : Всесоюз. ин-т по изучению причин и разраб. мер предупреждения преступности, 1984. – С. 36.

[2] Образцов В. А. О криминалистической классификации преступлений / В. А. Образцов // Вопр. борьбы с преступностью. – М., 1980. – Вып. 33. – С. 94.

[3] Яблоков Н. П. Обстановка совершения преступления как элемент его криминалистической характеристики / Н. П. Яблоков // Криминалистическая характеристика преступлений : сб. науч. тр. – М., 1984. – С. 38–39.

[4] Там само. – С. 38–39.

Обстановка розголошення професійних таємниць має своєю фундаментальною особливістю порушення стану інформаційної безпеки окремих суспільних відносин, що утворились у зв'язку із здійсненням певної професійної діяльності окремою особою, установою або організацією. Відомості про якість забезпечення стану інформаційної безпеки на час учинення злочину мають важливе криміналістичне значення, тому що вони надають важливі дані про окремі обставини, що сприяли або ж, навпаки, перешкоджали вчиненню злочину, та про особливості забезпечення безпеки предмета злочинного посягання, про характер взаємодії осіб під час здійснення певної професійної діяльності.

Інформаційна безпека відносно визначеної галузі професійної діяльності передбачає такий рівень організації та захисту інформаційних ресурсів, а також ступінь професійної підготовки працівників, який би забезпечував захист інформаційних ресурсів та інформаційних потоків від несанкціонованого доступу до них та порушення їх конфіденційності. Отже, обстановку розголошення професійних таємниць внаслідок особливого предмета злочинного посягання необхідно досліджувати, аналізуючи стан забезпечення інформаційної безпеки, конкретного інформаційного простору, в якому було розголошено професійну таємницю. Зокрема, розголошення професійних таємниць учиняється внаслідок недоліків у забезпеченні інформаційної безпеки певної професійної діяльності, на рівні *інформаційних ресурсів*, *інформаційної інфраструктур*и та «*інформаційного поля*»[1]. Аналіз названих рівнів дозволить виявити обставини та недоліки інформаційної безпеки, які сприяли чи перешкоджали вчиненню злочину щодо розголошення таємниці.

[1] Розуміння інформаційної безпеки в аспекті забезпечення безпеки інформаційних ресурсів, безпеки інформаційної інфраструктури, а також безпеки «інформаційного поля» було запропоновано А. І. Марущаком у дослідженні проблем забезпечення інформаційної безпеки банків (див.: Марущак А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези доп. Міжнар. наук.-практ. конф. (м. Севастополь, 1–2 жовт. 2010 р.) / А. І. Марущак ; Держ. вищ. навч. закл. «Укр. акад. банк. справи Нац. банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 21–24).

Розголошення професійних таємниць вчиняється через існування певних недоліків та негативних обставин у забезпеченні *безпеки інформаційних ресурсів*[1] і утворює перший рівень обстановки вчинення досліджуваної категорії злочинів. Указаний рівень включає недоліки та прорахунки в організації конфіденційності діловодства, кадрового, інформаційно-аналітичного та матеріально-технічного забезпечення безпеки інформаційних ресурсів у певній галузі професійної діяльності, що зумовили розголошення професійної таємниці. Сучасні дослідження свідчать, що організаційні заходи забезпечення інформаційної безпеки є найбільш вразливими у будь-якій системі забезпечення інформаційної безпеки[2]. Розголошення професійних таємниць учиняється як за умов відсутності спеціального діловодства, так і за умов неналежного рівня його організації та контролю за виконанням. Зокрема, мова йде про відсутність визначення строків, порядку зберігання та утилізації інформації з обмеженим доступом, або ігнорування чи недбале ведення журналу реєстрації фактів доступу до інформації з обмеженим доступом[3].

Цікавим є те, що у західних країнах, не дивлячись на серйозні досягнення у галузі програмного забезпечення запобігання витокам

[1] Під інформаційними ресурсами установи розуміють взаємопов'язану, упорядковану, систематизовану і закріплену на матеріальних носіях інформацію, яка або була надана до певної установи, організації у зв'язку зі здійсненням нею певної діяльності, або належить їй. Відповідно безпека інформаційних ресурсів полягає у збереженні такої інформації від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності) (див.: Марущак А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези доп. Міжнар. наук.-практ. конф. (м. Севастополь, 1–2 жовт. 2010 р.) / А. І. Марущак ; Держ. вищ. навч. закл. «Укр. акад. банк. справи Нац. банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 21).

[2] Исследование утечек информации и конфиденциальных данных из компаний и госучреждений России в 2012 г. [Электронный ресурс] : отчет об уровне защиты конфиденц. данных, 2013. – С. 13. – Режим доступа: http://www.infowatch.ru/node/3013?sid=5358. – Загл. с экрана.

[3] Близнюк І. Л. Основні засади політики безпеки банку : тези доп. Міжнар. наук.-практ. конф. (м. Севастополь, 1–2 жовтня 2010 р.) / І. Л. Близнюк ; Держ. вищ. навч. закл. «Укр. акад. банк. справи Нац. банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 47.

конфіденційної інформації, величезна кількість випадків «компрометування даних», тобто порушення їх конфіденційності, пов'язана саме з паперовими носіями та резервними копіями такої інформації. Отже, проблема полягає не стільки у відсутності певних програмних засобів захисту інформації, скільки у недостатньому рівні регламентації порядку роботи працівників з інформацією, а також їх низькій обізнаності у галузі забезпечення інформаційної безпеки, що, безумовно, становить суттєві недоліки організаційної складової захисту інформації[1]. Така необізнаність працівників викликає недбале поводження працівників із документами або машинними носіями, які містять певну професійну таємницю. Вказані дії можуть бути вчинені як з необережності, так й умисно, хоча, за оцінками фахівців, сьогодні близько ¾ від усіх витоків конфіденційних даних є ненавмисними – внаслідок помилок, недолугості, легковажності працівників. Проте варто пам'ятати, що оголошений факт «випадкового» витоку певної інформації може бути способом маскування вчиненого злочину, тобто спробою «легалізації» розголошеної інформації[2]. Усе зазначене обумовлює необхідність ретельного добору майбутніх кадрів, функціональні обов'язки яких пов'язані зі збором та опрацюванням конфіденційної інформації. При цьому необхідно враховувати психологічні особливості інсайдера – працівника, який здійснює певний тип професійної діяльності. Зокре-

[1] Исследование утечек информации и конфиденциальных данных из компаний и госучреждений России в 2012 г. [Электронный ресурс] : отчет об уровне защиты конфиденц. данных, 2013. – С. 16. – Режим доступу: http://www.infowatch.ru/node/3013?sid=5358. – Загл. с экрана.

[2] Так, працівник однієї з медичних мереж клінік (США) продав конфіденційні дані щодо пацієнтів. Розуміючи, що факт витоку незабаром виявиться, коли ці дані почнуть використовувати конкуренти, він інсценував «випадковий витік». Звернувся до поліції і заявив, що невідомі викрали ноутбук з інформацією з його автотранспорту. Заяву прийняли, провадження відкрили, факт витоку інформації отримав офіційний статус і вважався «неумисним», про що сповістили постраждалих осіб. Інсайдер мав усі шанси на успіх, він обмежився б дисциплінарним стягненням, якби на нього не вказав через півроку інший інсайдер – з конкурентної фірми, яка й придбала цю інформацію (див.: Федотов Н. Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? [Электронный ресурс] / Н. Н. Федотов. – Режим доступа: http://forensics.ru/investigation_blogs.html. – Загл. с экрана).

ма, майже всі різновиди професійних таємниць утворюються внаслідок активної професійної діяльності, яка передбачає взаємодію з іншими людьми (наприклад, лікарі, слідчі, банківські працівники тощо). Внаслідок такої взаємодії у працівників виникає особливий психологічний стан, який у психології отримав назву «емоційного згорання»[1], що необхідно враховувати. Окрім цього, науковці пропонують попередньо перевіряти надійність працівників (інсайдерів), які працюватимуть з інформацією обмеженого доступу, під час прийняття їх на роботу. Так, С. І. Журін зазначає, що перевірка має відбуватись за допомогою психологічних тестів, поліграфа, даних із попереднього місця роботи, співбесіди та ін.[2]

Вельми поширеною обставиною, яка сприяє розголошенню професійних таємниць, є відсутність диференційованого доступу[3] працівників до інформації, що становить професійну таємницю. За оцінками спеціалістів з інформаційної безпеки банківських установ, сьогодні доступ до будь-яких інформаційних активів мають майже всі співробітники банку, у тому числі й ті, яким за родом діяльності вони не потрібні[4], що, звісно, не забезпечує збереження певної інформації у таємниці. Розголошенню професійних таємниць сприяють й інші недоліки у забезпеченні стану безпеки інформаційних ресурсів певної професійної діяльності, зокрема, недостатній рівень обмеження доступу працівників або сторонніх осіб до приміщень, в яких обробляється (зберігається) інформація з обмеженим досту-

[1] Стан «емоційного згорання» виявляється у такому різновиді професійної деформації, як професійна індиферентність, що передбачає прояв байдужості, емоційної сухості, жорстокості, а також негативного сприйняття етичних норм і правил поведінки (див.: Зеер Э. Ф. Психология профессий : учеб. пособие / Э. Ф. Зеер. – 2-е изд., перераб., доп. – М. : Академ. Проект ; Екатеринбург : Делов. кн., 2003. – С. 114–115).

[2] Журин С. И. Инсайдер: основная характеристика и комплексность противодействия [Электронный ресурс] : науч. журн. ВНИИПВТИ «Безопасность информационных технологий» / С. И. Журин. – 2011. – № 4. – С. 178. – Режим доступа: http://www.pvti.ru/articles_34.htm. – Загл. с экрана.

[3] Під диференційованим доступом розуміємо той стан захисту інформації, за якого працівник може ознайомитись та опрацювати певні дані, виключно для виконання покладених на нього функціональних обов'язків.

[4] Курило А. Инсайдер – портрет на фоне банка дело в Москве [Электронный ресурс] / А. Курило, В. Голованов. – Режим доступа: http://www.abiss.ru/upload/iblock/b4a/insider.pdf. – Загл. с экрана.

пом[1]; відсутність заходів контролю за роботою працівників із носіями професійної таємниці; низький рівень дисципліни та професійні деформації працівників; відсутність ефективної системи виявлення та реагування на протиправні дії відносно інформації, яка становить професійну таємницю; ненадійна система охорони та зберігання носіїв інформації з обмеженим доступом (неналежний технічний стан сейфів, сховищ тощо), що не виключає можливість несанкціонованого ознайомлення з нею.

Другий рівень дослідження обстановки розголошення професійних таємниць становлять недоліки у забезпеченні *безпеки інформаційної інфраструктури*[2], які призвели до розголошення таємниці. Цей рівень включає недоліки та прорахунки у функціонуванні та забезпеченні безпеки використання «нових» інформаційних технологій, що включають комп'ютерні технології, зокрема, засоби обчислювальної техніки (комп'ютери) та програмне забезпечення, а також телекомунікаційні засоби зв'язку, які використовуються у певній галузі професійної діяльності. Серед недоліків інформаційної інфраструктури, які сприяють розголошенню професійних таємниць, можна назвати, зокрема, відсутність або незадовільний стан технічних засобів забезпечення безпеки інформаційної інфра-

[1] Наприклад, нормативно-правовими актами України передбачені вимоги щодо технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи з грифом «Банківська таємниця», а також окремі вимоги до систем електроживлення та заземлення, мережевого обладнання, приміщень з обмеженим доступом, комутаційних кімнат (приміщень, у яких розміщене телекомунікаційне устаткування, що забезпечує функціонування локальних і корпоративних мереж банку, а також зв'язок з іншими установами та мережами загального користування), серверних приміщень та приміщень, у яких зберігаються електронні архіви (див.: Близнюк І. Л. Основні засади політики безпеки банку : тези доп. Міжнар. наук.-практ. конф. (м. Севастополь, 1–2 жовт. 2010 р.) / І. Л. Близнюк ; Держ. вищ. навч. закл. «Укр. акад. банк. справи Нац. банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 47).

[2] Безпека інформаційної інфраструктури передбачає певний стан захищеності електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку певної установи, що забезпечують цілісність і доступність інформації, що в них обробляється (зберігається чи циркулює) (див.: Марущак А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези доп. Міжнар. наук.-практ. конф. (м. Севастополь, 1–2 жовт. 2010 р.) / А. І. Марущак ; Держ. вищ. навч. закл. «Укр. акад. банк. справи Нац. банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 21).

структури; фрагментарність або несправність засобів захисту, технічного і програмного середовища; відсутність криптографічного захисту для найбільш цінної інформації при її обробці у комп'ютерах (ЕОМ), системах та комп'ютерних мережах і мережах електрозв'язку певного підприємства; відсутність ідентифікації користувача та здійснюваних ним операцій з використанням комп'ютерів (ЕОМ) та комп'ютерних мереж за допомогою спеціальних паролів, ключів, магнітних карт, цифрового підпису при доступі до інформаційно-телекомунікаційних систем; неналежний рівень реєстрації, зокрема, відсутність відображення дати та часу дій користувачів з інформаційними та програмними ресурсами у комп'ютерах (ЕОМ), системах та комп'ютерних мережах, у тому числі і протиправних спроб доступу до них; відсутність програмного забезпечення, що розпізнавало б передачу інформації з обмеженим доступом незахищеними лініями зв'язку[1]. Так, у випадках надсилання конфіденційної інформації за допомогою комп'ютерної техніки (ЕОМ) та комп'ютерних мереж, окрім «людського» контролю, можливо здійснити й автоматизований контроль[2]. Так, спроба опублікувати в глобальній комп'ютерній мережі конфіденційну інформацію або відправити її у незашифрованому вигляді виявляється за допомогою *DLP-систем*[3].

---

[1] Марущак А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези доп. / А. І. Марущак ; «Укр. акад. банк. справи Нац. банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 23.

[2] Федотов Н. Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? [Электронный ресурс] / Н. Н. Федотов. – Режим доступа: http://forensics.ru/investigation_ blogs.html. – Загл. с экрана.

[3] DLP-системи (від англ. Data Leak Protection або Data Leak Prevention). Ці програмні засоби також іменуються ILP – Information Loss Protection, або ILDP – Information Leak Detection & Prevention. DLP-системи ефективно використовуються як для попередження, так і виявлення вже вчиненого розголошення. Так, розголошення професійних таємниць можливо виявити за допомогою вивчення існуючих публікацій у глобальній мережі. Виявляються такі публікації під час аналізу окремих матеріалів за допомогою пошукових систем, зокрема, шляхом формулювання до них кількох запитів, що містять потрібні ключові слова (див.: Федотов Н. Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? [Электронный ресурс] / Н. Н. Федотов. – Режим доступа: http://forensics.ru/investigation_blogs.html. – Загл. с экрана).

Третій рівень включає недоліки в безпеці «*інформаційного поля*» певної установи або організації, яке складається здебільшого з несистематизованих потоків інформації, які оприлюднюються різноманітними учасниками інформаційних відносин (телерадіоорганізаціями, друкованими ЗМІ, Інтернет-виданнями тощо)[1]. Слушно зауважує М. М. Федоров, що приймати рішення про коректність інформації, що надається до ЗМІ, може лише уповноважена особа – піар-цензор, який не лише є відповідальним за попереднє ознайомлення працівників з існуючою внутрішньою цензурою й реально контролює будь-яке спілкування, зокрема із ЗМІ[2].

У криміналістичній характеристиці злочинів щодо розголошення професійних таємниць набувають певної специфіки такі структурні компоненти, як *місце* та *час* вчинення злочинів. По-перше, місце вчинення розголошення професійних таємниць безпосередньо залежить від предмета злочинного посягання – професійної таємниці, форм її відображення у дійсності. Так, названі таємниці можуть існувати у вигляді матеріально-фіксованої інформації (письмові документи, роздруковані фотографії, креслення тощо) чи бути ідеально відображені у пам'яті осіб, або ж взагалі мати електронно-цифрове відображення (в пам'яті ЕОМ, на машинному носії інформації тощо). Це справляє вплив на обрання інсайдером місця вчинення, готування та приховування досліджуваної групи злочинів. По-друге, місце вчинення злочину залежить від різновиду обраного інсайдером способу доведення таємниці до відома сторонньої особи. Так, система вчинюваних дій з незаконного обміну інформацією відбувається за допомогою різних способів та засобів (мовленнєвих, технічних тощо), що обумовлює обрання інсайдером місця вчинення злочину. Найчас-

[1] Марущак А. І. Інформаційна безпека банківської установи: структура та система забезпечення : тези доп. Міжнар. наук.-практ. конф. (м. Севастополь, 1–2 жовт. 2010 р.) / А. І. Марущак ; Держ. вищ. навч. закл. «Укр. акад. банк. справи Нац. банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 23.

[2] Федотов Н. Н. Расследование инцидентов ИБ: Как расследовать разглашение конфиденциальной информации в блогах и форумах? [Электронный ресурс] / Н. Н. Федотов. – Режим доступа: http://forensics.ru/investigation_ blogs.html. – Загл. с экрана.

тіше місцем розголошення професійних таємниць є певне *матеріальне середовище*. Для злочинів щодо розголошення професійних таємниць характерні два типи місця їх вчинення. Зокрема, перший тип включає місця, *пов'язані зі здійсненням інсайдером своїх професійних обов'язків*, а саме робоче місце особи, певний кабінет чи окрема робоча зона на підприємстві, установі або організації. Робоче місце інсайдера, як правило, є місцем зберігання або опрацювання інформації, що становить предмет злочинного посягання, у зв'язку з цим воно часто стає місцем вчинення злочину. На робочому місці особа вчиняє дії з готування, вчинення чи приховування злочину. Проте ситуація змінюється, коли розголошення таємниці відбувається у *віртуальному просторі* за допомогою використання комп'ютерної техніки (ЕОМ) та комп'ютерних мереж. У названих випадках місце вчинення злочину буде обумовлене або місцем знаходження самої комп'ютерної техніки (ЕОМ), або місцем зберігання та обробки комп'ютерної інформації. До другої групи місць розголошення професійних таємниць належать *місця, не пов'язані з місцем роботи професійного інсайдера*. За таких умов, як правило, інсайдер отримує (збирає, копіює тощо) інформацію з обмеженим доступом на підприємстві або установі, де він працює. Проте безпосереднє її розголошення вчиняються поза роботою, зокрема, у певній неформальній обстановці, в якій відбувається зустріч інсайдера зі сторонньою особою.

Час учинення злочинів щодо розголошення професійних таємниць можливо охарактеризувати в трьох аспектах. По-перше, як момент безпосереднього розголошення професійної таємниці, тобто певний конкретно встановлений час (аж до хвилин). Встановлення настільки точного часу розголошення на сьогодні можливе лише у небагатьох випадках, зокрема, якщо інсайдер розголосив професійну таємницю, використовуючи комп'ютерну техніку (ЕОМ) чи комп'ютерні мережі або за допомогою засобів телекомунікаційного зв'язку. Використання зазначених засобів супроводжується утворенням електронно-цифрових слідів, які можуть надати дані щодо точного часу цих дій. При цьому

О. В. Курман слушно зазначає, що часовий чинник у досліджуваних злочинах може характеризуватись як роками, так і кількома хвилинами[1]. Так, розголошення професійних таємниць вчиняється як у робочі години з 9 до 18 год., так й у позаробочий час. Зокрема, М. О. Новікова зазначає, що основна маса розголошень таємниці слідства (90%) вчиняється у робочий час (з 9 до 18 год.)[2]. По-друге, час розголошення професійних таємниць можна охарактеризувати як певний період часу, протягом якого вчиняються розголошення професійних таємниць, тобто йдеться про кілька окремих епізодів діяння, які мають місце протягом певного періоду часу.

Таким чином, обстановка розголошення професійних таємниць має специфічний характер через особливий предмет злочинного посягання – інформацію з обмеженим доступом, що становить професійну таємницю, і впливає як на час, так і на місце вчинення злочину. Обстановка розголошення професійних таємниць характеризується порушенням стану інформаційної безпеки певної професійної діяльності, що призводить до розголошення професійної таємниці. У зв'язку з цим обстановка зазначених злочинів включає недоліки у забезпеченні інформаційної безпеки певної професійної діяльності на трьох самостійних рівнях, зокрема, на рівнях безпеки інформаційних ресурсів, безпеки інформаційної інфраструктури, а також безпеки «інформаційного поля». Таке розуміння сутності обстановки вчинення злочинів, предметом яких виступає професійна таємниця, дозволяє комплексно проаналізувати різнорідні недоліки у забезпеченні інформаційної безпеки, а також попередити у майбутньому факти розголошення інформації з обмеженим доступом.

---

[1] Курман О. В. Про криміналістичну характеристику злочинів, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю / О. В. Курман // Теорія та практика судової експертизи і криміналістики : зб. наук. пр. / ХНДІ суд. експертиз ім. М. С. Бокаріуса ; Нац. юрид. акад. України ім. Ярослава Мудрого. – Х. : Право, 2012. – Вип. 12. – С. 49–50.

[2] Новикова М. А. Расследование разглашения данных предварительного расследования и сведений о мерах безопасности, применяемых в отношении участников уголовного судопроизводства : автореф. дис. … канд. юрид. наук : 12.00.09 / М. А. Новикова ; Акад. управления МВД России. – М., 2009. – С. 13–14.

В статье анализируются особенности обстановки разглашения профессиональных тайн. Сосредотачивается внимание на отдельных недостатках, которые способствуют разглашению профессиональных тайн. Исследуется время и место совершения преступлений, связанных с разглашением профессиональных тайн.

This article is analyzed the specific environment of the disclosure of the professional secrets. The attention is paid on specific the shortcomings that contribute to disclosure of the professional secrets. The time and place of crimes against disclosure of professional secrets are researched

Рекомендовано до опублікування на засіданні лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» НДІ ВПЗ імені академіка В. В. Сташиса НАПрН України (протокол № 3 від 12 грудня 2013 р.).
Рецензент – доктор юридичних наук, професор, академік НАПрН України ***В. Ю. Шепітько****.*