політичні (шпигунство, діяння, спрямовані на підрив фінансової і грошово-кредитної політики, валютної системи країни); дослідницький інтерес; хуліганські спонукання і бешкетництво; помста тощо.

На сьогодні комп'ютерні злочини – це одна з найбільш динамічних груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Варто зауважити, що український законодавець приділяє значну увагу цій проблемі: Кримінальний кодекс України передбачив самостійний розділ про ці злочини – розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж»; двічі положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві.

Полуніна Лілія Валентинівна, старший викладач кафедри фінансових розслідувань факультету підготовки, перепідготовки та підвищення кваліфікації працівників податкової міліції Університету державної фіскальної служби України

ТАКТИКА ДОПИТУ ПІДОЗРЮВАНОГО ПІД ЧАС РОЗСЛІДУВАННЯ РОЗГОЛОШЕННЯ КОМЕРЦІЙНОЇ АБО БАНКІВСЬКОЇ ТАЄМНИЦІ

Сьогодні з'явилися нові, раніше невідомі способи злочинів у сфері підприємництва та конкурентних відносин, що зумовлює необхідність розроблення ефективних методик виявлення й розслідування цих кримінальних правопорушень.

Згідно зі ст. 36 Господарського кодексу України відомості, пов'язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб'єкта господарювання, можуть бути визнані його комерційною таємницею. Склад і обсяг відомостей, що

становлять комерційну таємницю, спосіб їх захисту визначаються суб'єктом господарювання відповідно до закону. Інформація становить комерційну таємницю за наявності таких ознак: 1) має дійсну або потенційну комерційну цінність через необізнаність з нею третіх осіб; 2) до неї не існує вільного доступу на законних підставах; 3) власник або уповноважена ним особа вживає заходів щодо збереження її конфіденційності.

Інформація, що складає комерційну таємницю, повинна бути зафіксована на матеріальному носії (папері, магнітному чи оптичному носії, фотонегативі чи іншому матеріальному об'єкті) та забезпечена реквізитами, що дозволяють її ідентифікувати. Це можуть бути: результати дослідів і їх протоколи, дані про якість матеріалів, документація з виготовлення продукції, креслення, формули та рецепти, статистичні розрахунки, звіти про виготовлену продукцію або надані послуги, картотеки й електронні бази даних клієнтів, відомості про організацію виробництва, методи реклами, інформація про джерела фінансування тощо.

У деяких ситуаціях інформація, що становить комерційну таємницю, може втілюватися в предметах: виробах, блоках, агрегатах, приборах і речовинах. Однак і в цьому разі для визнання відомостей, утілених у предметах, комерційною таємницею необхідно, аби інформація була попередньо задокументована в установленому порядку.

Банківською таємницею вважається інформація щодо діяльності й фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банку й розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Банківською таємницею, зокрема, є: 1) відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України; 2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; 3) фінансово-економічний стан клієнтів; 4) системи охорони банку та клієнтів; 5) інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрямки діяльності; 6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

7) інформація стосовно звітності по окремому банку, за винятком тієї, що підлягає опублікуванню; 8) коди, які використовуються банками для захисту інформації; 9) інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду.

Стаття 232 КК України визначає протизаконним також умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності.

Можна виділити декілька груп осіб, які потенційно можуть займатися незаконним збиранням і використанням інформації, що становить комерційну або банківську таємницю: 1) працівники підприємств, установ, організацій – конкурентів; 2) працівники, які займаються збиранням інформації на замовлення, знаходячись із власником комерційної таємниці (уповноваженим органом) у трудових відносинах; 3) працівники, які займаються збиранням інформації для себе (про всяк випадок); 4) особи, професійна або службова діяльність яких чи інші законні підстави зумовлюють виникнення певних правовідносин цивільно-правового характеру з власником комерційної таємниці; 5) особи, наділені власними повноваженнями з витребуванням і/або використанням відомостей, що становлять комерційну або банківську таємницю (наприклад, судді, працівники поліції, Служби безпеки України, прокуратури, митниці та ін.). Таку інформацію ці особи отримують, користуючись своїм службовим становищем не для виконання власних функцій, а для передання конкурентам чи використання в інших протиправних цілях, наприклад, різних видів шантажу щодо здійснення чи нездійснення певних дій за нерозголошення комерційної або банківської таємниці.

Способи розголошення комерційної або банківської таємниці можуть бути різними: усно, письмово, із застосуванням засобів зв'язку, повідомленням у засобах масової інформації, наукових статтях, шляхом умисного створення умов для ознайомлення з відповідними документами або предметами тощо.

Суб'єкт злочину – спеціальний. Ним є особа, якій комерційна або банківська таємниця стала відомою у зв'язку з професійною або службовою діяльністю. Крім працівників (у тому числі колишніх) суб'єктів господарювання організацій і фізичних осіб – підприємців, виконавцями аналізованого злочину можуть визнаватися працівники банківських установ, нотаріуси, особи, які виконують на певному підприємстві чи в його інтересах свої професійні обов'язки (наприклад, аудитор, адвокат, представник органів із сертифікації продукції), працівники податкових, правоохоронних та інших державних органів, які мають доступ до комерційної чи банківської таємниці у зв'язку з виконуваними службовими обов'язками.

Суб'єктом злочину може бути особа: 1) якій відповідна таємниця стала відома внаслідок її особливих взаємовідносин з власником таємниці (наприклад, член спостережної ради, інша посадова особа господарського товариства, яка не є його працівником, співвласник відповідної юридичної особи тощо); 2) яка є працівником юридичної особи чи індивідуального підприємця – власника таємниці; 3) яка є службовою особою органу державної влади (зокрема слідчим, прокурором, суддею) і отримала відповідні відомості на підставі закону під час виконання своїх службових обов'язків.

До осіб, яким комерційна таємниця стала відома у зв'язку з їх професійною або службовою діяльністю, слід відносити також працівників суб'єктів господарювання – контрагентів власника комерційної таємниці, оскільки в процесі спільної господарської діяльності вони можуть отримати відповідну інформацію, а, отже, здатні розголосити її з корисливих чи інших особистих мотивів.

Слідчі дії при розслідуванні злочинів у сфері господарської діяльності проводяться з дотриманням загальних процесуальних норм і рекомендацій криміналістичної тактики.

Слідчий використовує всі вербальні та невербальні тактичні засоби. Разом з тим деякі слідчі дії відрізняються специфікою, такі як допит, огляд і попереднє дослідження документів. Допит спрямований на встановлення безпосереднього предмета розголошення, його об'єму, виду та стану; способу розголошення чи зловживання; осіб, які брали

участь у цих операціях, їх способу життя, майнового стану, оточення та іншої інформації, яка зацікавить слідство.

Допит підозрюваних рекомендується проводити негайно, тільки у разі затримання з доказами. При цьому доцільно використовувати ефект раптовості. В інших випадках не слід поспішати, оскільки без зібраних доказів, що викривають, важко сподіватися на об'єктивні показання підозрюваного. Слідчий, готуючись до допиту підозрюваного, повинен зібрати достатню кількість доказової інформації, забезпечити базу свідків. Тільки тоді можна приступати до допиту, використовуючи всі рекомендовані прийоми тактики для викриття підозрюваного, викриття його в неправдивих показань та встановлення об'єктивної істини.

Пред'явлення підозрюваному доказів і даних є ефективним тактичним прийомом для викриття підозрюваного у неправдивих показаннях. При цьому можуть бути використані тільки перевірені, достовірні факти.

При допиті підозрюваного слідчий має за мету встановити: 1) що являє собою інформація, що вийшла із законного володіння (характеристика, зовнішні ознаки, наявність відомостей, що становлять комерційну або банківську таємницю тощо); 2) хто є відповідальною особою за збереження комерційної або банківської таємниці; 3) яка причина виходу інформації; 4) місце, час, спосіб здійснення розголошення таємниці.

Крім того, під час допиту підозрюваного слідчому необхідно мати на увазі, що останній має, як правило, вищу освіту та володіє спеціальними знаннями. Ця обставина вимагає від слідчого необхідності поглибленого вивчення матеріалів кримінального провадження; нормативних актів, що регламентують порядок зберігання, розголошення комерційної та банківської таємниці; ознайомлення із спеціальною літературою; отримання консультацій від фахівців із певних галузей знань або навіть вирішення питання щодо їх залучення до проведення допиту; визначення послідовності епізодів, щодо яких буде допитаний підозрюваний.

Дослідження особливостей проведення допиту підозрюваного під час розслідування комерційної або банківської таємниці має важливе значення для розроблення

методики розслідування злочинів, пов'язаних із посяганнями на відомості, що становлять комерційну або банківську таємницю. Знання тактики проведення слідчої дії дозволяє слідчому встановити технології та злочинні механізми посягань, висунути версії, визначити напрями розслідування, побудувати оптимальні комплекси наступних слідчих (розшукових) дій.

Самарський Ярослав Вікторович, курсант навчально-наукового інституту № 2 Національної академії внутрішніх справ
Науковий керівник: кандидат юридичних наук, завідувач кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ ***Атаманчук В. М.***

МОЖЛИВОСТІ ВИКОРИСТАННЯ ПОЛІГРАФА: СУЧАСНИЙ СТАН І МІЖНАРОДНИЙ ДОСВІД

Зараз, більше ніж коли-небудь, співробітники правоохоронних органів починають розуміти, що боротьба зі злочинністю стала менш ефективна при використанні старих, традиційних методів. Організована злочинність для підготовки і здійснення злочинів нерідко використовує останні досягнення науки і техніки, щоб одержати важливу для себе інформацію. У своєму арсеналі злочинці мають сучасні підслуховуючи пристрої, системи перехоплення радіо- і телефонних сигналів, дистанційно знімають інформацію з дисплеїв комп'ютерів, у складних умовах із застосуванням сучасних технічних засобів ведуть візуальне спостереження. Щоб успішно їм протидіяти, технічне оснащення міліції повинно бути на дуже високому рівні.

Одним із технічних пристроїв, що дозволяють прискорити процес викриття злочинця, є детектор брехні (поліграф).

Перевірки на поліграфі засновані на фіксації й інтепретації психофізіологічних реакцій людського організму на