Підрозділ 11.2. Сучасні інформаційно-комунікаційні технології у правовій сфері

Ємельянов С. Л.
Національний університет «Одеська юридична академія»,
завідуючий кафедрою правової інформатики,
кандидат технічних наук, доцент

ПРОБЛЕМА ФОРМУВАННЯ ПРАВОВИХ ІНСТИТУТІВ ТАЄМНИЦЬ В УКРАЇНІ

Одним з перших і достатньо важливих етапів комплексного дослідження об'єкту інформатизації на предмет інформаційної безпеки є інвентаризація інформаційних ресурсів і виявлення інформації, що повинна захищатися. Стосовно забезпечення конфіденційності інформації цей етап може здійснюватися, наприклад, експертним методом на основі встановлення відповідності інформації, циркулюючої на об'єкті, переліку відомостей, які відносяться до одного із законодавчо передбачених видів таємниць.

Згідно до чинного законодавства (Закон України «Про інформацію» в ред. від 13.01.2011 р., Закон України «Про доступ до публічної інформації» від 13.01.2011 р) за порядком (режимом) доступу інформація поділяється на відкриту та інформацію з обмеженим доступом (ІзОД). У свою чергу, ІзОД поділяється на конфіденційну, таємну та службову інформацію. До таємної належить інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю.

Прагнення України увійти у світовий інформаційний простір як його повноправний учасник зумовлює актуальність проблеми побудови правових інститутів таємниць (ПІТ) та оцінки їх ефективності задля збереження балансу публічних і приватних інтересів, забезпечення жорсткого і надійного режиму захисту важливої інформації в поєднанні із недоторканністю законних прав і інтересів громадян.

Різні аспекти цієї складної та багатогранної проблеми розглядались як російськими (І. Л. Бачило, В. А. Копилов, В. Н. Лопатін, М. М. Рассолов та ін.), так і вітчизняними (В. М. Брижко, К. І. Бєляков, Р. А. Калюжний, Є. А. Макаренко, О. В. Соснін, В. С. Цимбалюк, М. Я. Швець, С. О. Янішевський та ін.) науковцями.

Правовий інститут будь-якої таємниці можна умовно представити у вигляді трьох взаємопоєднаних складових: загальна частина (визначення таємниці, принципи та критерії віднесення інформації до таємниці, обмеження щодо включення певної інформації до таємниці, правові ознаки таємниці тощо); режим таємниці (правовий механізм обмеження доступу

до інформації, що складає таємницю); санкції (юридична відповідальність за протиправні дії з інформацією, що складає таємницю).

Сукупність правових норм, яка регламентує інформаційні відносини у сфері обігу інформації, що складає таємницю, і утворює окремий правовий інститут, оскільки їй властиві однорідність фактичного змісту, єдність правових норм.

Зазначимо, що до правових інститутів, що регулюють сукупність однорідних суспільних відносин, пов'язаних із обігом ІзОД, та мають усі зазначені складові зараз відносять інститути: державної таємниці (ДТ), банківської таємниці (БТ); комерційної таємниці (КТ), професійної таємниці (ПТ); захисту персональних даних (Виноградова Г. В. Правове регулювання інформаційних відносин в Україні: Навчальний посібник. 2006, с.10.).

Кількісна оцінка якості законодавчого забезпечення вказаних правових інститутів може бути здійснена на підставі факторно-критеріальної моделі (ФКМ) (Ємельянов С. Л. Методика та результати оцінки якості законодавчого забезпечення правового інституту таємниць в Україні // Вісник СНУ ім. В. Даля. – м. Луганськ. 2011. № 7(161), с.57-62).

Згідно вказаної моделі оцінка якості ПІТ визначається як сукупність факторів та критеріїв, що інтегрально впливають на неї, та які оцінюються експертним шляхом, зокрема: чіткість законодавчого визначення таємниці; порядок та критерії віднесення інформації до таємниці; обмеження на інформацію, що може складати таємницю; наявність окремого нормативно-правового акту, що регулює обіг таємниці; ступень нормотворчої активності (зміни до законів, законопроекти, концепції реформування законодавства тощо);. чіткість правових ознак таємниці;

регламентація порядку засекречування, обігу та розсекречування таємниці; наявність грифів обмеження доступу; рівень правової охорони державою; встановлення юридичної відповідальності за протиправні дії з інформацією, що складає таємницю (за діючими Кодексами України); ступень активності правозастосовчої діяльності (судова практика); взаємоузгодженість загальної частини таємниці, правового механізму її захисту та санкцій за протиправні дії щодо інформації, яка містить таємницю.

Вказаний підхід дозволив визначити якість законодавчого забезпечення вищезгаданих ПІТ та виявити певні недоліки у їх побудові та функціонуванні (Ємельянов С. Л. Проблемні аспекти організаційно-правового захисту державної таємниці в Україні // Інформаційна безпека. – м. Луганськ. 2011. Вип. 1(5), СНУ ім. В. Даля, с.36-44; Ємельянов С. Л. Проблемні аспекти організаційно-правового захисту банківської таємниці в Україні // Право і безпека. 2011. № 3(40), с.194-199; Ємельянов С. Л. Проблемні аспекти організаційно-правового захисту комерційної таємниці в Україні // Інформаційна безпека. м. Луганськ. 2011. Вип. 2(6),

СНУ ім. В. Даля, с.37-45; Ємельянов С. Л. Стан та розвиток правового інституту професійної таємниці в Україні // Право і безпека. 2012. № 5 (42), с.52-57; Ємельянов С. Л. Проблемні аспекти розкриття банківської таємниці в Україні // Вісник СНУ ім. В. Даля. – м. Луганськ. 2012. № 8(179), с.150-157).

Вказані дослідження показали, що високий рівень законодавчого забезпечення має правовий інститут ДТ (95 %). Правові інститути БТ (53 %), КТ (65 %) та СТ (50 %) мають лише базовий рівень забезпечення (від 50 % до 75 %); ПТ має задовільний рівень правового забезпечення (47 %). Фактично це означає, що держава створила дієві правові інститути зазначених таємниць, проте існуючі механізми їх правового захисту ще мають багато недоліків. ПІТ інших видів таємниць знаходяться лише у стадії становлення та мають незадовільний рівень правового забезпечення (до 25 %).

Якутко В. Ф.

Национальный университет «Одесская юридическая академия», доцент кафедры правовой информатики, кандидат технических наук, доцент

СПОСОБЫ СНИЖЕНИЯ ДОСТОВЕРНОСТИ ПОЛИГРАФНЫХ ПРОВЕРОК

Полиграф – устройство, предназначенное для психофизиологических исследований синхронно регистрирующее изменения определённых физиологических параметров человека, при ответе на поставленный вопрос, с представлением результатов регистрации в виде полиграммы. Анализ полиграммы позволяет оценить правдивость информации полученной в ходе полиграфной проверки и представить результат проверки в виде заключения. На достоверность результатов полученных в ходе полиграфных проверок влияет множество различных факторов, которые полиграфолог должен знать и учитывать в своей работе.

Понятие «достоверность» означает вероятность определения истины при полиграфной проверке. При этом в равных условиях правомерно ожидать постоянства получаемых результатов. Степень такого постоянства, при сохранении неизменных условий самой проверки, определяет достоверность полиграфной проверки. Если проверка на полиграфе достоверна, то при последующих проверках должен достигаться одинаковый результат – вывод об истинности (или лживости) ответов проверявшегося.

Последние исследования показывают, что правильность выводов квалифицированных полиграфологов составляет 98 %. Исследования подтверждают то, что при проведении полиграфной проверки компетентным полиграфологом, проверка на полиграфе даёт достаточно достоверные результаты при определении правды и лжи. Использование полиграфа в