Використані джерела:

1. О.О. Чуприна, К.С. Чуприн Методологічні підходи до оцінювання інтелектуального капіталу// Вісник Національного університету «Юридична академія України імені Ярослава Мудрого» № 3 (14) 2013. [Електронний ресурс] Режим доступу: http://econtlaw.nlu.edu.ua/wp-content/uploads/2016/01/3-22-34.pdf
2. Давос-2019: главные месседжи Всемирного экономического форума. Экономическая правда [Електронний ресурс] Режим доступу: www.epravda.com.ua/rus/publications/2019/01/27/644694/
3. Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики. Аналітична записка. Національний інститут стратегічних досліджень. [Електронний ресурс] Режим доступу: http://old2.niss.gov.ua/articles/1191/

Гупал Д. курсант факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник: Рижков Е.В.
к.ю.н. , доцент, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ З ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З метою протидії злочинності, ефективного попередження, припинення та розкриття злочинів органи та підрозділи Національної поліції України здійснюють необхідні: слідчі (розшукові) дії; негласні слідчі (розшукові) дії; оперативнорозшукові дії. Під час підготовки та проведення зазначених дій працівники поліції використовують інформацію з обмеженим доступом в акустичному та електронному вигляді [1, с. 20].

Така інформація може циркулювати в акустичному вигляді під час проведення нарад щодо планування певних негласних заходів. В електронному вигляді інформація циркулює, наприклад, під час підготовки необхідних документів, таких як плани, звіти, клопотання до суду.

Дана інформація може бути цікавою для представників організованих злочинних груп, та, навіть, представників іноземних розвідок. Вони можуть отримати доступ до цієї інформації шляхом фізичного доступу на об'єкт де циркулює ця інформація (в службовому кабінеті працівника поліції).

Також за допомогою сучасних приладів зловмисники можуть аналізувати

бездротові мережі (Wi-Fi) та вилучати незаконним методом данні жертви. Сучасні засоби технічної розвідки дозволяються підключатися дистанційно до обчислювальних машин, створювати перешкоди у телекомунікаційних каналах між пристроями і супутниковою системою, бездротових мережах [2].

В разі отримання несанкціонованого доступу сторонніх осіб до інформації з обмеженим доступом, це може призвести до більш ефективної протидії злочинців щодо документування їх діяльності з боку працівників правоохоронних органів або неможливості затримання злочинців.

З метою не допущення витоку інформації з об'єктів інформаційної діяльності поліції необхідно вживати заходів з технічного захисту інформації, таких як періодичний пошук засобів негласного зйому інформації («закладних пристроїв») та використання технічних засобів захисту акустичної інформації та електронно-обчислювальних машин.

На сьогоднішній день на ринку представлено багато різних за призначенням та технічними можливостями технічних засобів пошуку та захисту інформації, як українського так і закордонного виробництва. При цьому періодично на ринку з'являються нові розробки та нові технічні засоби.

Під час вибору технічних засобів, що будуть використовуватися для забезпечення захисту інформації, слід звернути увагу на такі технічні засоби як:

1. Тепловізори – використовуються для виявлення пристроїв, що виділяють температурне поле. Зазвичай ці прилади приховуються зловмисником у стінах.

2. Багатофункціональні пошуковий прилади – зазвичай вони поєднують в собі широкосмуговий детектор електромагнітного поля, приймач інфрачервоного діапазону, різні додаткові зонди для перевірки провідних ліній і оцінки віброакустичного захисту приміщення [3, с. 102].

3. Частотоміри – дозволяють виміряти частоту сигналу безконтактно, за допомогою антени. Така властивість дозволяє застосовувати їх як для замірів «відомих» сигналів, так і для пошуку «прихованих» сигналів від підслуховуючих пристроїв (жучків).

Таким чином, можна зробити висновок, що для забезпечення захисту інформації з обмеженим доступом від витоку з об'єктів інформаційної діяльності Національної поліції можуть використовуватися різноманітні технічні засоби, як пошукові та засоби захисту інформації.

Використані джерела:

1. Красіков Д.О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.19 К., 2019. - 20 с.

2. Іванець Т.М. Інформаційев безпека держави як умова для збереження національного суверенітету. [Електронний ресурс] Режим доступу: http://intkonf.org/ivanets-tm-informatsiyna-bezpeka-derzhavi-yak-umova-dlya-zberezhennyanatsionalnogo-suverenitetu/ (дата звернення: 12.11.2020).

3.Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України № 537V від 9 січня 2007 р. Відомості Верховної Ради України. 2007. № 12. Ст. 102.