# ИСПОЛЬЗОВАНИЕ ПРОСЛУШИВАЮЩИХ УСТРОЙСТВ В ДЕЯТЕЛЬНОСТИ ОВД И ИХ ЗНАЧЕНИЕ В КАЧЕСТВЕ ДОКАЗАТЕЛЬСТВ

THE USE OF LISTENING DIVICES IN THE ACTIVITIES OF THE INTERNAL AFFAIRS BODIES AS EVIDENCE

**Смирнов Виталий Михайлович,** к.т.н., старший преподаватель кафедры информатики и математики Московского университета МВД имени В. Я. Кикотя, г. Москва

**Дрокина Полина Романовна,** курсант Московского университета МВД имени В. Я. Кикотя, г. Москва

**Smirnov V.M.** smirnov.v.m.002@gmail.com

**Drokina P.R.** Drokina.p@mail.ru

**Аннотация**

В статье рассматривается понятие информационной безопасности, а также применение технических прослушивающих устройств в деятельности правоохранительных органов. В ходе расследования разного рода дел сотрудники правоохранительных органов используют современные технические средства, в число которых вошли и прослушивающие устройства. Их использование помогает вычислить преступника и вовремя не допустить совершения преступления. Можно сказать, что такие средства необходимы в арсенале ОВД. Прослушивание, которое осуществляют сотрудники ОВД в рамках расследования, не всегда бывает легитимным, хотя при этом результаты этого по большей части эффективны.

**Annotation**

The article discusses the concept of information security, as well as the use of technical listening devices in the activities of law enforcement agencies. During the investigation of various cases, law enforcement officers use modern technical means, including listening devices. Their use helps to identify the criminal and prevent the commission of a crime in time. We can say that such funds are necessary in the arsenal of the Department of Internal Affairs. Eavesdropping carried out by internal affairs officers as part of an investigation is not always legal, although the results are mostly effective.

**Ключевые слова:** прослушивание, основания, связанные с нарушениями, оперативные сотрудники, цифровые технологии.

**Keywords:** eavesdropping, grounds related to violations, operational staff, digital technologies.

Сегодня нельзя отрицать то обстоятельство, что информационно – телекоммуникационные технологи стремительно развиваются и совершенствуются. При этом происходящие социальные явления можно назвать непростыми, более того, сложными. Среди таких явлений есть весьма опасные. Это обусловлено тем, что современные информационные технологии на сегодняшний день развиваются крайне стремительно. Такая динамичность не всегда правоохранительным органам позволяет использовать их в своей работе.

Таких угроз сегодня очень много. Со своей стороны правоохранительные органы должны реагировать на них быстро и интенсивно. В данном случае речь идет об информационной безопасности и, соответственно, о пресечении такого рода преступлениях и не только. Здесь имеется ввиду то, обеспечение информационной безопасности, прежде всего, возложено на правоохранительные органы.

Понятие информационной безопасности очень ёмкое и имеет разные дефиниции, которые по большей части схожи.

Например, можно сказать, что под информационной безопасностью, как правило, подразумевают определённые мероприятия, позволяющие закрыть

доступ к важным или секретным данным чужим и посторонним лицам. Так, ещё задолго до того, как появились существующие сегодня цифровые технологии, такую информацию нужно было защищать и охранять. Для этого в организациях использовали надёжные сейфы, работали охранники, кроме того, если информация была крайне секретной, её приходилось зашифровывать.

Или другое определение информационной безопасности. Это «всесторонняя защищённость информации и поддерживающей её инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий»[1].

В ходе расследования разного рода дел сотрудники правоохранительных органов используют современные технические средства, в число которых можно отнести и прослушивающие устройства. Их использование помогает вычислить злоумышленника и вовремя не допустить совершения преступления. Безусловно, такие средства необходимы в арсенале ОВД.

Часто на практике при расследовании уголовных дел разговоры по телефону фигурантов прослушивались, но в деле они появлялись незаконно, так как прослушивание переговоров осуществлялось с нарушением правовых норм и в рамках расследования другого уголовного дела, поэтому эти записи являются недопустимыми доказательствами. Можно сказать, что такие записи нельзя использовать как доказательства.

Прослушивание может быть проведено и вне рамок судебного решения. Вне всяких сомнений нужно исключать из числа доказательств диски с переговорами и все производные от этого доказательства. В частности, заключения фоноскопической и психолого-лингвистической экспертиз.

---

[1] Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019. с. 78

Если комментировать теоретическую сторону этого вопроса (законно ли использовать в материалах дела записи телефонных разговоров, если же они были получены в рамках другого расследования), то на этот вопрос однозначного ответа нет, все зависит от тонкостей дела. То есть, в общей сложности эта ситуация решается так: суд должен проверить законность любого доказательства, которое рассматривается в деле: его возникновение, получение, то, как оно попало в дело. На все это есть свои правила. Если это доказательство получено по другому делу, то должна прослеживаться процессуальная цепочка, почему оно оказалось в другом деле.

Это должно быть обосновано определенными процессуальными решениями, предусмотренными законом: выделение дел, соединение дел, поскольку ситуации могут возникать разные. Если все эти требования выполнены, и действительно нет нарушений, то в принципе такое можно себе представить. Но если один материал просто взяли из одного дела и присоединили их к другому без законных оснований, то он не может рассматриваться в качестве доказательства.

Нередко прослушивание, которое осуществляют сотрудники ОВД в рамках расследования, не всегда бывает законным, хотя при этом результаты этого по большей части эффективны. Об этом можно часто встретить статьи и иные материалы в СМИ или интернете.

Нельзя не допускать, что практика такие вещи принимает, в других случаях суды, вероятно, могли такое делать раньше. Как представляется, все зависит от дела и конкретной ситуации. То есть, записи переговоров по телефону, полученные в рамках одного дела, скорее всего, признавали допустимым доказательством в другом деле. Но это совершенно не означает, что в этом конкретном случае все было сделано корректно, потому что это не так, что нельзя делать то, что незаконно.

Следствие должно процессуально держаться в требуемых рамках, а это не всегда проходит гладко, и возможно, что в конкретном случае будут основания, связанные с нарушениями, которые были допущены в ходе этой процедуры

перекладывания из одного дела в другое. Несмотря на то, что суды эту практику применяют, это совершенно не означает, что при этом выдерживаются все соответствующие требования. Есть такие вещи как европейская конвенция. С точки зрения конвенции далеко не очевидно, что разрешение, которое давал суд на запись и прослушивание по одному делу, может быть использовано в другом деле.

Как известно, результаты ОРД часто фальсифицируются. Но факт этого сложно доказать и в общем – то и не целесообразно, поскольку такие результаты обычно оцениваются несколько иначе, чем другие, фигурирующие в деле доказательства, иными словами, все прослушанные разговоры касательно лиц, проходящих по делу, могут быть представлены в самом выгодном свете для следователя, и лишь те, что представляют для дела интерес.

Следует добавить ко всему вышеизложенному, что оперативные сотрудники ОВД могут передать материалы прослушивания в ИФНС для оценки их экономической составляющей. В случае с уголовными статьями следственные органы и налоговые органы действуют вместе. При этом, налоговая инспекция выступает в суде в качестве пострадавшей стороны. Материалы прослушивания «ложатся» в доказательную базу стороны обвинения.

**Список литературы**

1. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.- Екатеринбург: Изд-во Урал. ун-та, 2019.— 204 с.
2. Осипенко А.Л., Лахин А.Н. Использование информационных технологий в деятельности оперативных подразделений органов внутренних дел // Вестн. Волгоград. акад. МВД России. 2016. № 2(37).
3. Луговик В.Ф., Осипенко А.Л. Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования // Вестн. Воронеж. ин-та МВД России. 2015. № 4.
4. Международный конгресс по кибербезопасности. Тематическая сессия «Киберпреступность – на шаг впереди?». URL: https://icc.moscow/translyatsii.html

5. Ларина Е., Овчинский В. Реформа полиции в Америке времен Трампа: превентивное реагирование, цифровой мир и главная проблема полиции в XXI веке. URL: http://zavtra.ru/blogs/reforma_politcii_v_amerike_vremyon_trampa

**List of references**

1. Fundamentals of information security: a textbook for university students / E.V. Vostretsova. - Yekaterinburg: Ural Publishing House. University, 2019.— 204 p.
2. Osipenko A.L., Lakhin A.N. The use of information technologies in the activities of operational units of internal affairs bodies // Vestn. Volgograd. acad. Ministry of Internal Affairs of Russia. 2016. No. 2 (37).
3. Lugovik V.F., Osipenko A.L. Operational-search activity of internal affairs bodies: prospects for improving legal regulation // Vestn. Voronezh. Institute of the Ministry of Internal Affairs of Russia. 2015. No. 4.
4. International Congress on Cybersecurity. Thematic session "Cybercrime - one step ahead?" URL: https://icc.moscow/translyatsii.html
5. Larina E., Ovchinsky V. Police reform in America during the Trump era: preventive response, the digital world and the main problem of the police in the XXI century. URL: http://zavtra.ru/blogs/reforma_politcii_v_amerike_vremyon_trampa