AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
"TƏFƏKKÜR" UNİVERSİTETİ

HÜQUQİ ELMLƏR VƏ TƏHSİL

JURNALI

ЖУРНАЛ

ЮРИДИЧЕСКИЕ НАУКИ И ОБРАЗОВАНИЕ

№ 18

BAKI—TƏFƏKKÜR—2005

Молчанов С.Г.,
аспирант Белорусского государственного университета
Гучок А.Е.,
прокурор отдела Прокуратуры Республики Беларусь,
кандидат юридических наук, доцент

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМЕ ПРОТИВОДЕЙСТВИЯ ВЗЯТОЧНИЧЕСТВУ

Взяточничество является одним из самых опасных и распространенных коррупционных составов. Трудности расследования взяточничества связаны с его высокой латентностью, а также достаточно специфическими и в то же время скудными в информационном плане следовыми картинами. Специфика криминалистической структуры взяточничества определяется количеством входящих в нее элементов (взяткодателей, взяткополучателей, посредников) особенностями предмета взятки (денежные средства, материальные ценности, услуги и т.п.), а также результатами выполнения взяткополучателем обязанностей перед взяткодателем воплощенными в материальном виде (предоставление жилого или иного помещения) либо не в материальном (оказание медицинских услуг). Особенности криминалистической структуры взяточничества определяют специфику познавательной деятельности в ходе производства расследования по делам данной категории. При этом познавательная деятельность осуществляется посредством криминалистического анализа каждого элемента криминалистической структуры взяточничества и всей системы взяточничества в целом.

Необходимо обратить внимание, что в ходе совершения взяточничества одним из специфических элементов данного вида преступлений является информация. Она может выступать в качестве объекта "купли - продажи" на рынке коррупционных услуг. В связи с этим, в качестве одного из направлений антикоррупционной деятельности должна рассматриваться разработка и внедрение систем защиты информации. Противодействие коррупции посредством использования таких систем следует ориентировать на минимизацию или исключение возможности "продажи" чиновниками различной информации с одной стороны и нецелесообразность ее "покупки" с другой.

Следует отметить, что защита информации предполагает с одной стороны исключение возможности ее искажений, и с другой стороны сведение к минимуму прецедентов ее полного игнорирования. При этом в широком смысле информация представляет собой сведения о лицах, предметах, фактах, событиях, явлениях и процессах (1). Таким образом, налицо необходимость разработки подходов, не допускающих искажение сведений, или исключающих возможность уничтожения информации, которая касается отдельных фактов, событий, явлений и процессов.

Учитывая определение информации, предложенное Н. Винером в работе "Кибернетика и общество" "Информация - это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств" (2, с. 61), можно утверждать о том, что объектом исследования должна выступать в первую очередь система соответствующих обозначений того содержания, которое представляет интерес. При этом наше приспособление к внешнему миру и приспособление к нему же наших чувств в эпоху технократического общества окончательно привело к тому, что одним из обязательных элементов в деятельности по обозначению и, что наиболее важно для правоохранительной деятельности, фиксации информации, используемой в правоохранительной деятельности, на сегодняшний день, стали технические средства.

Таким образом, полагаясь на точку зрения Н. Винера о том, что "процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде" (2, с. 61), необходимо констатировать, что технические средства выявления и фиксации информации стали как раз и средствами ее получения, и средствами ее использования. При этом, не выпуская из виду то, что информация - результат взаимодействия данных (зарегистрированных сигналов) и адекватных им методов следует принимать в учет и необходимость совершенствования методологии выявления необходимой информации, т.е. разработки конкретно адекватных интересующим данным методов, обеспечивающих эффективность их выявления, достоверность фиксации и, самое главное, необходимую сохранность.

Одним из наиболее важных объектов исследования в сфере правоохранительной деятельности вообще и деятельности по противодействию коррупции выступает оперативно-розыскная информация. "Оперативно-розыскная информация включает знания о явлениях, которые свидетельствуют о преступной деятельности конкретных лиц и раскрывают не только механизм преступлений, но и механизм возникновения информации о них" (3, с. 61). Отметим, что само по себе наличие каких-либо результатов взаимодействия данных, без соответствующего их обозначения, обязательно сопряженного с их восприятием и фиксацией, даже если эти данные содержат информацию о преступлении и его участниках, не представляет собой не только оперативно-розыскной или криминалистически значимой информации, но и не является информацией вообще. Именно это позволяет в ходе преступных действий коррупционного характера либо не воспринимать определенные результаты взаимодействия данных вообще, с целью не получения какой-либо информации, либо не фиксировать эти данные, либо зафиксировав, исключать их взамен за соответствующее вознаграждение.

На основе этого и определяются основные подходы, направленные на совершенствование системы защиты информации на обозначенных стадиях. Положительный опыт в этой части может быть получен путем анализа информационной сущности фиксации доказательств.

"Информационная сущность фиксации доказательств заключается в том, что:

а) производится перекодировка доказательственной информации, содержащейся в ее материальном носителе и перенос ее на средство фиксации;

б) обеспечивается сохранение доказательственной информации для неоднократного использования в процессе доказывания;

в) обеспечивается возможность накопления информации до пределов, выражающих полное установление предмета доказывания, т.е. до момента доказанности всех входящих в него обстоятельств;

г) получает свое материальное выражение отбор информации о событии: фиксируется не вся информация, поступающая к следователю и суду, но лишь:

- относящаяся к предмету доказывания (относимая информация);
- допустимая законом (допустимая информация);
- существенная с точки зрения предмета доказывания;

д) запечатлевается не только сама доказательственная информация, но и сведения о путях, способах ее получения как необходимое условие признания ее допустимости по делу" (4, с. 148-149).

Необходимо указать, что наиболее эффективным способом защиты информации является ее фиксация с немедленным исключением доступа к ней с целью ее изменения или уничтожения.

Наиболее ярким примером в этой части служит работа ДПС ГАИ по контролю за скоростью движения транспортных средств. Анализируя работу инспекторов ДПС можно предположить, что информация о факте превышения скорости движения транспортного средства может выступать в качестве специфического объекта "купли - продажи" и составлять один из элементов рынка коррупционных услуг. Так, зафиксировав превышение скорости движения транспортных средств с помощью радар-детектора и предъявив показания данного прибора нарушителю, инспектора могут получить предложение исключить за соответствующее вознаграждение общий порядок привлечения нарушителя к административной ответственности. Результатом договоренности между сотрудником ДПС и водителем нарушителем может стать не привлечение последнего к ответственности. Это возможно за счет уничтожение (сброса) информации зафиксированной радар-детектором.

Одним из наиболее перспективных технических средств контроля скорости является внедрение радара "Искра-1" совместимого с видеофиксатором "Кадр-1" и персональным компьютером. Использование указанного технического комплекса позволяет осуществлять визуальный контроль дорожной обстановки, регистрацию фактов нарушений ПДД, предоставление документальной информации. Видефиксатор "Кадр-1" дает возможность осуществлять многократное фотографирование дорожной ситуации (2 кадра в секунду), автоматическое внесение в кадр скорости нарушителя, даты и времени, данных о режимах измерения, а также номера прото-

кола об административном правонарушении. Отснятые кадры записываются в оперативную память и, далее, при необходимости обеспечения доказательственной базы переносятся в архивную память прибора. Однако следует отметить, что при работе с радаром "Искра-1" и видеофиксатором "Кадр-1" инспектор ДПС ГАИ имеет возможность исключить "нежелательную" информацию о нарушении правил ПДД путем удаления отснятых кадров-файлов из памяти прибора.

Следует обратить внимание, что опыт зарубежных стран свидетельствует о невозможности в настоящее время проявления аналогичных прецедентов в их работе. Разрешение такого рода проблем осуществляется путем установки систем контроля скорости, работающих в автоматическом режиме.

Аналогичные системы нашли применение и в работе ГИБДД Российской Федерации. Так, например, фоторадар "Крис-1" контролирует скоростную обстановку в автоматическом режиме, формирует базу данных нарушителей и обеспечивает дистанционный обмен данными с центральным постом или другим внешним компьютером (например, установленным на патрульном автомобиле). Однако, и в этом случае информация о превышении максимальной допустимой скорости не защищена и может быть удалена работниками ГИБДД непосредственно на компьютере.

Отметим, что данные технические средства не находят широкого распространения в Республике Беларусь в связи с высокой стоимостью и значительными затратами на их эксплуатацию. Кроме того, такие установки эффективно выполняют свои функции лишь на определенных участках дорог, осведомленность водителей о которых становится достаточно быстрой. Следует указать и на большую эффективность проведения операций "Скорость" именно экипажами ДПС с использованием радар-детекторов.

Проблема защиты информации о нарушении скоростного режима движения и невозможности ее использования в преступной деятельности может быть решена посредством исключения функции сброса показателей радар-детектора с момента получения прибора при отбытии на несение службы к месту проведения мероприятия, до момента его сдачи с одновременным копированием информации на CD-R. При этом количество взысканий, наложенных на водителей нарушителей должны соответствовать количеству фактов превышения скорости, зафиксированных радар-детектором.

Одним из наиболее совершенных способов защиты информации в данном случае является внедрение средств электронной цифровой подписи. Правоотношения, складывающиеся в сфере использования средств электронной цифровой подписи и электронного документооборота урегулированы законом Республике Беларусь "Об электронном документе". Электронная цифровая подпись предназначена для:

- удостоверения информации, составляющей общую часть электронного документа;
- подтверждения подлинности и целостности электронного документа (5).

Так, при фиксации инспектором ДПС с помощью радара "Искра-1" и ви-

деофиксатора "Кадр-1" дорожной обстановки информация не содержащая сведений о фактах превышения скорости накапливается в оперативной памяти и в необходимых случаях может быть удалена. Если с помощью названных технических средств запечатлены факты нарушения скоростного режима, то по нашему мнению данная информация должна автоматически записываться в архивную память и прибора и сохраняться в ней будучи защищенной от сброса (удаления) цифровой подписью начальника подразделения ДПС. Дифференциация фактов превышения скорости осуществляется путем установки на приборе значения допустимой скорости движения на заданном участке дороги. В данном случае компьютерный файл, созданный в архивной памяти средства фиксации дорожной обстановки, служит основой для создания электронного документа, который, согласно отечественному законодательству, должен отвечать следующим требованиям:

- создаваться, обрабатываться, передаваться, и храниться с помощью программных и технических средств;
- быть представленным в форме, понятной для восприятия человеком;
- иметь установленную законодательством структуру и реквизиты, позволяющие ее идентифицировать (5).

При подобном подходе факт нарушения скоростного режима, зафиксированный с помощью современных технических средств и наделенный электронной цифровой подписью, полностью соответствует предъявляемым требованиям и может использоваться в дальнейшем в практике работы ДПС ГАИ как электронный документ.

На основе изложенного примера считаем необходимым сделать вывод о том, что возможность применения данного подхода применительно к средствам фиксации любой оперативно-розыскной, криминалистической и иной информации, имеющей значение для разрешения уголовного, административного, гражданского дела должна быть изучена дополнительно. При этом в качестве средств защиты такого рода информации могут рассматриваться не только электронные устройства, исключающие возможность уничтожения или изменения информации зафиксированной на соответствующем носителе, но и уже известные способы, в частности электронные цифровые подписи.

БИБЛИОГРАФИЯ

1. Закон Республики Беларусь "Об информатизации" от 6 сентября 1995 г. № 3850-XII.

2. Винер Н. Кибернетика и общество. - М., 1958.

3. Овчинский С.С. Оперативно-розыскная информация. М., "ИНФРА-М", 2000.

4. Криминалистика: Учебник для вузов / Под ред. Р.С. Белкина. - М.: Издательство НОРМА, 2001.

5. Закон Республики Беларусь "Об электронном документе" от 10 января 2000 г. № 357-3.