Галимова А. Г., *преподаватель кафедры физической подготовки Восточно-Сибирского института МВД России (г. Иркутск);*
Медвежонков А. В., *курсант 4-го курса*

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА И ГОСУДАРСТВА

Современные темпы развития научно-технического прогресса, в том числе в сфере информационных систем, телекоммуникаций, а также систем связи, требуют нового отношения к вопросам национальной безопасности, особенно к так называемой информационной безопасности.

Совершенствование средств вычислительной техники представляет собой основу новой информационной технологии, которая применяется для создания комплексных автоматизированных систем информационного обеспечения, сводящих участие человека в этом процессе к минимуму (компьютер в автоматизированном режиме может производить собирание, передачу, обработку, хранение и выдачу необходимой информации).

В настоящее время защита информации от несанкционированного доступа и неправомерного завладения ею лицами либо организациями, которым она не принадлежит, может нанести огромный ущерб ее владельцу. Ущерб от таких неправомерных действий может затрагивать интересы, начиная от физических лиц, включая финансовое состояние крупных международных корпораций и заканчивая экономической стабильностью того или иного государства. Наиболее ярким примером такой утечки можно считать события, связаные с личностью Эдварда Джозефа Сноудена. По данным закрытого доклада Пентагона, «Сноуден похитил 1,7 млн. секретных документов, касающихся не только деятельности американских спецслужб, но и операций всех видов вооруженных сил США — сухопутных войск, ВВС, ВМС и морской пехоты»[1], а также были раскрыты факты всеобъемлющего слежения в 60-ти странах за более чем миллиардом человек, правительствами 35-ти стран. По данным некоторых источников, доля российских утечек информации в мировой статистике составляет приблизительно 6 % от общего количества утечек информации в мире. Данный показатель по сравнению с прошлым годом увеличился на треть, однако большинство фиксируемых утечек, приблизительно 36,9 %, является следствием человеческих ошибок или халатности, но не злого умысла. Что, впрочем, не исключает серьезности последствий.

Во все времена деятельность органов внутренних дел России в значительной мере связана с получением и использованием сведений ограниченного доступа, разглашение которых может повлечь нарушение конституционных прав граждан, а также снижение эффективности работы правоохранительных органов по предупреждению, раскрытию и расследованию преступлений. В процессе осуществления своей служебной деятельности сотрудники органов внутренних дел получают информацию о режиме и характере работы предприятий, расположенных на обслуживаемой территории, сведения, касающиеся личной жизни граждан, а также иную информацию (служебного либо личного характера). Данная информация, а также информация, связанная с тактикой и методикой работы правоохранительных структур системы МВД России, и результаты работы органов внутренних дел составляет служебную тайну. Утечка и уж тем более разглашение информации служебного характера о планируемых или проводимых органами внутренних дел мероприятиях по охране общественного порядка, информации, связанной с раскрытием и расследованием преступлений и иных правонарушений, может серьезно повлиять на эффективность деятельности ОВД России.

Умение сохранять в тайне сведения служебного характера является важнейшим профессиональным качеством сотрудника органов внутренних дел России, необходимым для успешного выполнения стоящих перед ним задач. При этом проявление высокой бдительности считается юридической обязанностью сотрудника органов внутренних дел России, закрепленной в законодательных и ведомственных нормативных актах. Однако некоторые сотрудники часто недооценивают опасность утечки таких сведений. Они проявляют

граничащую с преступной халатностью беспечность при обращении со служебными документами, что нередко приводит к их утрате и разглашению сведений служебного характера.

Сегодня МВД России придает огромное значение мерам по защите служебной информации. Однако недостатки в работе сотрудников ОВД, а также ограниченность правоприменительной практики, обеспечивающей должную защиту конфиденциальной информации служебного либо личного характера, не позволяют реализовывать механизм устранения имеющихся нарушений и привлечения виновных лиц к ответственности. И это в тот период, когда приоритетным направлением является развитие информационного обеспечения системы МВД России.

Примером утечки личных данных сотрудников системы МВД России является случай, произошедший в апреле 2012 г. недалеко от Казани. Инспекторы Центрального территориального управления министерства экологии обнаружили несанкционированную свалку. Среди мусора были найдены личные дела военнослужащих расквартированной неподалеку воинской части специального назначения МВД России. Ее бойцы являлись участниками контртеррористических операций на Северном Кавказе. Данный пример показывает безответственное отношение должностных лиц к своим обязанностям. В большинстве случаев утечки персональных данных были связаны с халатными или неосторожными действиями рядовых сотрудников или должностных лиц, а в некоторых случаях вина за утечку лежит на руководителях (средних и высших уровней). В более чем 50 % фактов наблюдается причинение ущерба в различной форме владельцу либо лицу, фигурировавшему в содержании данной информации.

В системе МВД России как раньше, так и в настоящее время наблюдается огромный оборот «бумаги», т. е. информации, находящейся на бумажном носителе, а по статистике утечка такой информации в 2013 г. составила приблизительно 25,4 % от общего количества утечек информации. Примером такой утечки может быть кража уголовного дела, как умышленно, так и вследствие совершения лицом другого противоправного деяния.

Рассматривая вопросы утечки информации, не стоит забывать и о ее защите, на которую были направлены неправомерные действия со стороны третьих лиц. Как уже было сказано ранее, информация, с которой «работают» сотрудники органов внутренних дел, имеет ограничительный гриф и требует качественной защиты. Рассматривая вопросы, связанные с защитой информации ОВД России, необходимо раскрыть такое понятие, как информационная безопасность ОВД. Под информационной безопасностью ОВД понимается состояние защищенности интересов ОВД в информационной сфере, определяющихся совокупностью сбалансированных интересов личности (сотрудников и др.), общества и государства (служебных, ведомственных).

Защите информации в ОВД России уделяется большое внимание и затрачиваются огромные силы, как в техническом, так и процессуальном отношении. Но, несмотря на большой объем нормативной базы информационной безопасности, как в гражданской, так и правоохранительной сфере существует проблема правоприменения, в связи с недостатком квалифицированных сотрудников в данной отрасли.

В настоящее время в системе ОВД России предпринимаются активные меры для повышения информационной защищенности объектов. Создаются защищенные каналы передачи данных, устанавливается необходимое программное обеспечение и т. д. Вместе с тем, необходимо уделять серьезное внимание подготовке кадров в области информационной безопасности, осуществлять подготовку специалистов данного профиля в вузах системы МВД Российской Федерации.

[1] Пентагон: Сноуден похитил секретные документы, касающиеся операций вооруженных сил США // http://itar-tass.com/mezhdunarodnaya-panorama/877984.