Становление службы технической защиты информации в УМВД России по Забайкальскому краю и основные направления ее развития

Карандаев Андрей Владиславович,
начальник отделения по противодействию техническим разведкам и технической защиты информации ЦИТСиЗИ УМВД России по Забайкальскому краю, майор внутренней службы

Стремительное развитие информационных технологий, широкое применение вычислительной техники, средств связи и телекоммуникаций привело к образованию единого информационного пространства и созданию общей системы правил поведения субъектов в информационной сфере. Конституция Российской Федерации, принятая в декабре 1993 года, провозгласила право на свободный поиск, получение, передачу, производство и распространение информации (ст. 29). В мае 2009 года Президентом Российской Федерации утверждена стратегия национальной безопасности Российской Федерации до 2020 года, в которой определены приоритеты национальной безопасности. Одним из таких приоритетов является деятельность по обеспечению государственной и общественной безопасности. В целях обеспечения реализации указанного приоритета необходимо укреплять режимы безопасного функционирования информационных систем на всех уровнях управления с соблюдением требований информационной безопасности. Полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру. Тем самым наличие и использование государственных информационных ресурсов, отнесенных законом к категории ограниченного доступа, предполагает наличие вполне определенного режима защиты, установленного соответствующими нормативно правовыми актами.

Защите подлежит информация, как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных сигналов, физических полей, носителей на бумажной, магнитной и иной основе. С целью исключения или существенного затруднения добывания информации техническими средствами разведки, а также предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней в процессе ее обработки и передачи в соответствии с приказом МВД России от 05 июля 2001 года № 029 «Об утверждении временного наставления по технической защите информации в органах внутренних дел Российской Федерации и внутренних войсках Министерства внутренних дел Российской Федерации», а также руководствуясь Положением о государственной системе защиты информации в Российской Федерации, утвержденного постановлением Совета Министров — Правительства Российской Федерации от 15 сентября 1993 года № 912–51, с учетом Типового положения о подразделении по защите информации на предприятиях (в учреждениях, организациях), одобренного решением Гостехкомиссии России от 14 марта 1995 года № 32, в МВД, ГУВД, УВД по субъектам Российской Федерации в штатной структуре подразделений связи было предписано создать подразделения по технической защите информации.

Можно считать, что именно с этого момента техническая защита информации стала новым направлением деятельности в УМВД России по Забайкальскому краю. Так, в штатной структуре отдела связи, специальной техники и автоматизации тогда еще в УВД Читинской области была создана группа защиты информации. В связи с отсутствием подготовленных специалистов указанного профиля справиться с организацией подразделения по защите информации было поручено старшему инженеру группы защиты информации отдела связи, специальной техники и автоматизации УВД по Забайкальскому краю капитану милиции Александру Сергеевичу Подопригора. Под его непосредственным руководством начали складываться первые так называемые «кирпичики» новой службы.

На вновь созданное подразделение были возложены функции организации и проведения работ по подбору и внедрению комплекса организационных (режимных) и технических мер по защите информации в соответствии с требованиями и рекомендациями в данной области, аттестации объектов информатизации органов внутренних дел Забайкальского края, ведомственный контроль за соблюдением установленных правил и требований безопасности информации при обработке сведений, составляющих государственную и служебную тайну.

Современные технологии создают возможность широкого внедрения в повседневную деятельность

средств и систем автоматизации различного уровня и назначения, а развитие единой информационно-телекоммуникационной системы в органах внутренних дел Российской Федерации, в свою очередь, резко снижает безопасность информации по ряду причин. Например:

- Значительно увеличиваются объемы информации, накапливаемой и хранимой в автоматизированных системах и средствах вычислительной техники. В создаваемых единых базах данных сосредотачивается информация различного уровня конфиденциальности;
- Расширяется круг лиц, имеющих доступ к средствам вычислительной техники;
- Происходит усложнение технологии обработки информации с применением электронного обмена в локально вычислительных сетях;
- Информация все чаще является товаром и объектом преступных посягательств.

Вопросы защиты информации требовали и требуют наличие в структуре территориальных органов внутренних дел высокопрофессиональной службы, укомплектованной компетентными специалистами. Поэтому одним из важнейших направлений деятельности на первоначальном этапе стало обучение назначаемых сотрудников современным методам и способам обеспечения информационной безопасности. Подготовка специалистов была проведена на курсах повышения квалификации в учебном центре ЦБИ г. Юбилейного по программам: 1. Аттестация объектов информатизации по требованиям безопасности информации. Защита от утечки по техническим каналам. 2. Аттестация объектов информатизации по требованиям безопасности информации. Защита от несанкционированного доступа. Также сотрудники прошли обучение в учебно-техническом центре «НОВОУТЦ» г. Москвы по программе «Организация и обеспечение работ по поиску и нейтрализации технических средств негласного получения информации». Руководящий состав отделения обучался на высших

академических курсах в Академии управления МВД России.

Полученные теоретические и практические навыки в области технической защиты информации позволили специалистам технической защиты информации компетентно разрабатывать организационно-распорядительные документы на объекты информатизации, умело решать поставленные перед ними задачи технической защиты информации.

В период 2001–2008 года организация деятельности по технической защите информации направлялась в основном на создание нормативно-правовой базы, разработку методических рекомендаций, внедрения организационных (режимных) мер на существующих объектах информатизации, подбор соответствующих кадров и увеличение штатной численности подразделения. В 2008 году на очередном заседании постоянно действующей технической комиссии по защите государственной тайны УВД по Забайкальскому краю было принято решение о введении дополнительных штатных единиц в существующее подразделение по защите информации и создании отделения по технической защите информации. После создания отделения начали формироваться организационные, методологические подходы к защите информации от технических разведок и от ее утечки по техническим каналам. Развернулась практическая работа по оказанию методической и практической помощи подразделениям органов внутренних дел Забайкальского края. Значимым направлением развития службы технической защиты информации является проведение единой технической политики по обеспечению данных подразделений современными сертифицированными техническими и программными средствами защиты информации, а также измерительным и специальным поисковым оборудованием.

Своего рода итогом деятельности по технической защите информации является аттестация объектов информатизации, предназначенных для обработки сведений, составляющих государственную и служебную тайны. По результатам аттестационных испытаний посредством специального документа — «Аттестата соответствия» — подтверждается, что объект соответствует требованиям стандартов и иных нормативно-тех-

нических документов по безопасности информации.

В связи с тем, что проводить аттестационные испытания могут только аккредитованные в Федеральной службе по техническому и экспортному контролю (ФСТЭК) России организации, значительные бюджетные средства уходят на оплату работ сторонних организаций. В целях решения этой проблемы следующим важным направлением развития деятельности по технической защите информации стало получение аттестата аккредитации ведомственного органа по аттестации объектов информатизации. Совместно с представителями ФСТЭК России по Сибирскому Федеральному округу сотрудниками отдела организации технической защиты информации УИТТиС Департамента тыла МВД России был разработан план мероприятий по получению лицензий ФСТЭК России на осуществление мероприятий и оказание услуг в области защиты государственной тайны.

В рамках подготовки к проведению специальной экспертизы на соответствие требований и условий по заявленному виду деятельности была проведена аттестация собственных объектов информатизации, необходимых для дальнейшего осуществления деятельности. При поддержке руководства УМВД России по Забайкальскому краю выделены финансовые средства на создание и ввод в эксплуатацию альтернативной измерительной площадки УВД по Забайкальскому краю, организован сбор и подготовка базы нормативно-методических документов, необходимых для осуществления деятельности по технической защите информации. Выполнены мероприятия по заключению договоров на использование недостающего измерительного оборудования.

Результатом данных мероприятий в 2009 году стало получение лицензий ФСТЭК России на осуществление мероприятий и оказание услуг в области защиты государственной тайны, а также получения Аттестата аккредитации ведомственного органа по аттестации. Создания собственного органа по аттестации позволило эффективнее организовывать аттестацию по требованиям безопасности информации органов внутренних дел Забайкальского края, проводить специальные исследования технических средств, что в конечном счете привело к существенной экономии финансовых средств и положительно повлияло на всю организацию служебно-оперативной деятельности подразделений.

В настоящее время существует еще ряд нерешенных задач, которые бы позволили в полном объеме выполнять все мероприятия по обеспечению информационной безопасности.

Приоритетными направлениями подразделения по технической защите информации остаются:

- совершенствование форм и методов по противодействию техническим разведкам и технической защите информации;
- совершенствование мер по обеспечению информационной безопасности;
- совершенствование работы в целях защиты сведений, составляющих государственную тайну, недопущения разглашения секретной и служебной информации;
- проведение аттестационных испытаний объектов информатизации с последующей их аттестацией;
- повышение профессионального уровня сотрудников органов внутренних дел в области технической защиты информации;
- получение лицензии Роспотребнадзора в области использования источников ионизирующего излучения, ФСБ России на оказание услуг по защите государственной тайны;
- взаимодействие с органами государственной власти по организации работы в области технической защиты информации.

К сожалению, организационно-штатные мероприятия, проводимые в МВД России, затронули и подразделение по технической защите информации, но сотрудники технической защиты информации УМВД России по Забайкальскому краю будут стараться идти в ногу со временем, внедряя новейшие образцы перспективной техники, привлекая квалифицированных специалистов в данной области с целью надежного обеспечения информационной безопасности.

И в заключение хотелось бы сказать, что созданный в рамках реформирования МВД России Департамент информационных технологий, связи и защиты информации (ДИТСиЗИ), одним из направлений которого является организация и координация мероприятий по защите информации, проведения единой технической политики в данной области, создание полноценных штатных подразделений на уровне МВД, ГУМВД, УМВД по субъектам Российской Федерации, под своим чутким руководством создаст мощную эффективную систему обеспечения информационной безопасности в органах внутренних дел Российской Федерации, что в конечном итоге станет принципиальным качественным шагом в становлении и развитии технической защиты информации.