Об информационном обеспечении участковых уполномоченных полиции в МВД по Республике Татарстан

Хуснуллин Фирдус Котдусович,
начальник отдела сопровождения видеонаблюдения и видеоконференцсвязи ЦИТСиЗИ МВД по Республике Татарстан, подполковник внутренней службы

Решение задач борьбы с преступностью, защиты прав и интересов граждан во многом зависит от новых, более эффективных форм и методов оперативно-служебной деятельности, соответствующих современному развитию общества.

Важнейшим шагом по развитию современных подходов к борьбе с преступностью и внедрению передовых информационных технологий стало создание Единой информационно-телекоммуникационной системы органов внутренних дел (далее ЕИТКС). Её использование уже сегодня предоставляет широчайшие информационные возможности — от моментального получения информации из специализированных баз данных федерального и регионального уровней до проведения видеоконференций и осуществления образовательных программ для сотрудников министерства.

С расширением внедрения вычислительной техники в различные сферы деятельности органов внутренних дел начался фактически новый этап развития информационных технологий — время безбумажной информатики с еще большим увеличением степени автоматизации всех информационных процессов. Компьютерная обработка информации способствует дальнейшему развитию интеллектуальных и аналитических функций правоохранительных органов в целом и ОВД в частности. Компьютер уже сегодня позволяет зарегистрировать происшествие, получить сведения о месте, времени, средствах и способах совершения преступлений, изъятых следах, месте жительства подозреваемых лиц и потерпевших, выявить структуру преступности по регионам, предприятиям, возрастным и социальным группам, создать свои, требуемые в работе конкретного сотрудника учеты и т.д.

Среди отраслевых служб, призванных защищать права граждан, интересы общества и государства от преступных и иных противоправных посягательств, охранять общественный порядок и обеспечивать общественную безопасность, важное место занимает служба участковых уполномоченных полиции. Функции данной службы составляют самое объемное и многообразное направление деятельности ОВД, осуществляемое в профилактических, непосредственно охранительных, административно-правовых и уголовно-процессуальных формах.

Отсутствие у участковых уполномоченных полиции возможности использования автоматизированных информационно-поисковых и адресно-справочных баз данных снижает уровень их упреждающего влияния на криминогенные процессы в местах проживания населения.

25 ноября 2010 года на всероссийском совещании в режиме видеоконференции, посвященном деятельности участковых уполномоченных милиции, на связь с руководством МВД России вышли участники Всероссийского совещания-семинара руководителей подразделений обеспечения деятельности участковых уполномоченных милиции, которое проходило в Омске. Министр внутренних дел России генерал армии Рашид Гумарович Нургалиев поручил руководителям МВД-ГУВД-УВД по субъектам Российской Федерации активизировать усилия по реализации комплекса мер, направленных на информатизацию деятельности участковых уполномоченных милиции с использованием инновационных технологий.

Важным этапом в организации деятельности участковых уполномоченных полиции по профилактике правонарушений является налаживание и функционирование системы информационного обеспечения, планирование ими деятельности в соответствии со складывающейся оперативной обстановкой и планами мероприятий горрайоргана внутренних дел. Осуществляя свою деятельность, участковый уполномоченный должен использовать значительное количество различных источников информации как во внутренней (по отношению к органам внутренних дел), так и во внешней среде. Собираемая информация должна носить комплексный характер и включать в себя значительный перечень вопросов — от демографической ситуации, социально-экономической обстановки на обслуживаемом участке до конкретных сведений о поведении состоящих на профилактическом учете лиц. Использование информации должно носить многоцелевой характер; участковый уполномоченный должен осуществлять целенаправленный ее сбор и анализ.

Встает резонный вопрос: как организовать автоматизированный доступ к различным источникам информации? В большинстве своем для участковых пунктов полиции и общественных пунктов охраны порядка (далее УПП и ОПОП) единственным доступным видом коммуникаций является телефонная связь общего пользования. Строить собственные или арендовать выделенные каналы связи в масштабах республики — мероприятие, требующее колоссальных финансовых затрат и поэтому неприемлемое. Остается вариант: это использование сети Интернет или сети, приравненной к ней (в Республике Татарстан это — ГИСТ, Государственная интегрированная система телекоммуникаций, о которой будет сказано ниже).

Представить какую-либо компанию, у которой отсутствует локальная сеть и нет доступа к Интернету, становится все сложнее и сложнее. С одной стороны — это обычная технология, позволяющая улучшить работу, обеспечить быстрый доступ к информации, обмену документами, данными. С другой стороны — при широком использовании сети Интернет возникает необходимость решения проблемы защиты информации и локальной сети в целом.

В 2004 году распоряжением Кабинета Министров Республики Татарстан было положено начало созданию ГИСТ. Ее целью является формирование единой сети органов управления, научно-образовательных организаций и учреждений бюджетной сферы. Система позволяет не только централизованно обеспечивать все органы власти доступом в сеть Интернет и к основным сервисам ГИСТ, но и гарантирует информационную безопасность. Сегодня узлы доступа в систему есть во всех городах и районах республики, что позволяет государственным структурам любого уровня оперативно и эффективно взаимодействовать. Такая возможность предоставляется в результате использования самых современных электронных средств связи и инфокоммуникационных технологий. Внедрение ГИСТ осуществляется наряду с развитием систем видеоконференцсвязи, региональных центров обработки и хранения данных, унифицированных коммуникаций в органах государственной власти, а также информационно-телекоммуникационной инфраструктуры.

ГИСТ и легла в основу среды передачи данных для доступа не только к ресурсам сети Интернет, на портал органов государственной и исполнительной власти (http://tatarstan.ru/http://tatarstan.ru/), но и к информационным ресурсам органов внутренних дел при условии использования технических средств защиты информации (далее ТСЗИ).

С целью защиты информации и предотвращения несанкционированного доступа в Центральном телекоммуникационном узле МВД по Республике Татарстан внедрён комплекс технических средств, обеспечивающих защищенный доступ пользователей к информационным базам данных, использующий внешние сети как транспортную среду. Комплекс состоит из межсетевого экрана, имеющего необходимые сертификаты, и сертифицированного по требованиям ФСБ и ФСТЭК России сервера шифрования данных в канале VipNet. Сервер выведен в так называемую «демилитаризованную зону» (далее — ДМЗ). ДМЗ — технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети (который и называется ДМЗ) и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана (файрвола) с целью минимизации ущерба при взломе одного из общедоступных сервисов, находящихся в ДМЗ.

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

В нашем случае в ряде УПП и ОПОП на имеющиеся телефонные линии установлены модемы сети передачи данных Центра информационных технологий Республики Татарстан, который осуществляет техническую поддержку ГИСТ.

На выделенный персональный компьютер для работы участкового уполномоченного полиции устанавливается [Клиент] — модуль, обеспечивающий защиту информации при ее передаче в сеть, защиту от доступа к ресурсам компьютера и атак на него из локальных и глобальных сетей, а также реализующий на каждом рабочем месте следующие функции: защищенные службы для организации

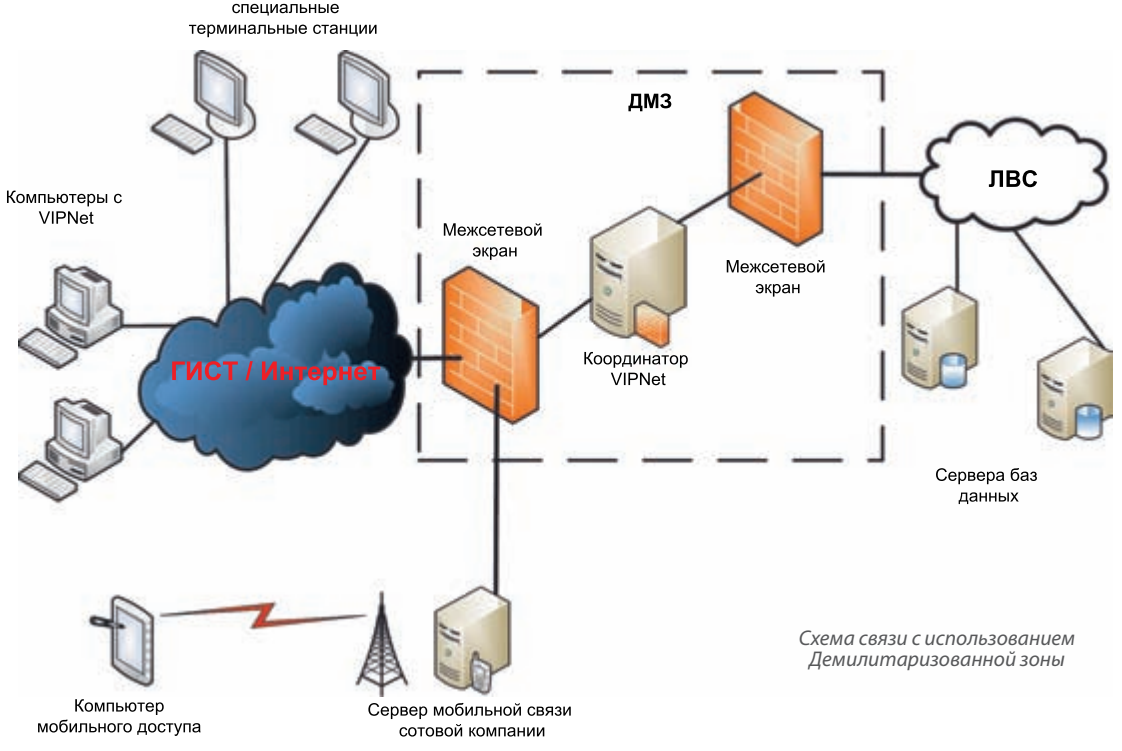

Схема связи с использованием Демилитаризованной зоны

циркулярного обмена сообщениями, проведения конференций, защищенную почтовую службу и др. Также данный модуль «вживлен» в специальные станции терминального доступа «тонкий клиент», которые в качестве эксперимента установили в некоторых ОПОП Казанского гарнизона полиции (фото 1 и 2). Не забыли также и о тех участковых, для которых нет технической возможности организовать доступ к информационным ресурсам по проводным видам связи. Для них приобретаются и выделяются компьютеры мобильного доступа, представляющие собой специализированное изделие с сенсорным экраном, встроенным 3G-модемом, исполненное в ударопрочном и влагозащищённом корпусе для удалённой работы полиции с информационными базами данных ОВД (АПК «Барс»).

Общественный пункт охраны порядка

Клиенты регистрируются на сервере [Координатор] в составе ДМЗ. [Координатор] — многофункциональный модуль, выполняющий следующие функции:

- маршрутизацию почтовых и управляющих защищенных сообщений при взаимодействии объектов сети между собой и ViPNet [Администратором];
- осуществление в реальном времени регистрации и предоставление информации о состоянии объектов сети, их местоположении, значении их IP-адресов и др.;
- обеспечение работы защищенных компьютеров локальной сети в VPN от имени одного адреса (функция proxy);
- туннелирование пакетов от обслуживаемой ViPNet [Координатором] группы незащищенных компьютеров локальной сети для передачи трафика от них к другим объектам VPN в зашифрованном виде по открытым каналам;
- фильтрацию трафика от источников, не входящих в состав VPN, в соответствии с заданной политикой безопасности (функция межсетевого экрана);
- обеспечение возможности работы защищенных по технологии ViPNet компьютеров локальной сети через сетевые экраны и прокси-серверы других производителей.


Рабочее место участкового уполномоченного полиции.

В результате проведенных мероприятий получены следующие результаты:

1. Образован защищенный сегмент сети МВД, доступ в который строго ограничен.
2. Получена единая контролируемая точка соприкосновения сети «Интернет» и приравненных к ней «внешних» ЛВС подразделений МВД с защищенным сегментом.
3. Установлена система обнаружения вторжений, обеспечивающая обнаружение, информирование, запись обо всех действиях, попадающих под понятие «сетевая атака».
4. Антивирусное сканирование проходящего трафика.
5. Сеть МВД по Республике Татарстан имеет четкую структуру, что обеспечивает быструю диагностику неисправности при возникновении, а также уменьшает вероятность её появления.
6. Возможность установки приоритета трафика и выделение определенной полосы пропускания.

Таким образом, у нас открываются широкие возможности по организации информационного взаимодействия не только в пределах органов внутренних дел, но и участие в системе межведомственного электронного документооборота, взаимодействие с органами исполнительной власти по вопросам информатизации, организации предоставления государственных услуг (исполнения государственных функций) в электронном виде, входящих в компетенцию МВД России.