

С.С. ЕПИФАНОВ, С.Н. КЛЕНОВ, В.В. ПОПОВ, А.А. ИВАНОВ

**СПЕЦИАЛЬНАЯ ТЕХНИКА ПРАВООХРАНИТЕЛЬНОЙ
ДЕЯТЕЛЬНОСТИ**
(теоретические, правовые и организационные аспекты)

Курс лекций

В курсе лекций рассматриваются теоретические, правовые и организационные вопросы применения специальной техники и обеспечения безопасности информации в деятельности сотрудников правоохранительных органов Российской Федерации.

Курс лекций предназначен для студентов, курсантов и слушателей образовательных учреждений правоохранительных органов России. Он может представлять интерес для научных сотрудников, аспирантов, адъюнктов и соискателей, а также для практических работников и специалистов в сфере применения специальной техники и информационной безопасности.

Рецензенты:

Н.С. Артемьев, Заслуженный работник высшей школы РФ доктор юридических наук, профессор (Рязанский государственный университет имени С.А.Есенина);

И.Н. Нуштин, кандидат юридических наук, доцент (Академия ФСИН России).

ISBN

© С.С. Епифанов, С.Н. Кленов, 2007

© Вологодский институт права и экономики ФСИН России, 2007

ПРЕДИСЛОВИЕ

Анализ состояния преступности за последние годы свидетельствует, что из-за коренного изменения социально-экономических условий в России она приобрела тенденцию общего роста и ухудшения своих качественных характеристик. Возникают и развиваются новые формы преступных проявлений, происходит дальнейшее оснащение криминальных структур современными техническими средствами, предназначенными для проведения как разведывательных действий, так и информационных атак и психологического воздействия в каналах информационного обмена.

Резко возросла общественная опасность преступности. Продолжают происходить дерзкие заказные убийства, разбойные нападения и грабежи. Похищение людей становится высокодоходным бизнесом. Угрожающие размеры приобрела контрабанда взрывчатых веществ, оружия и боеприпасов, совершаются чудовищные террористические акты. Незаконный оборот наркотиков принял общенациональные масштабы. Значительная часть экономического потенциала и финансовых ресурсов государства находится под контролем частных фирм, связанных с организованными преступными формированиями. Российская преступность стремительно выходит за рамки национальных границ, интегрируется в преступные транснациональные сообщества.

Сохраняется преследующая криминальные цели тенденция к активизации связей отрицательно настроенной части осужденных с криминалитетом вне мест лишения свободы для воздействия на управленческие структуры, конкретных руководителей и сотрудников уголовно-исполнительной системы.

В настоящее время для дезорганизации деятельности правоохранительных органов криминалитетом разрабатываются системы несанкционированного съема, добывания, анализа и обработки оперативно-служебной информации.

Развитие ситуации требует принятия незамедлительных, адекватных и решительных мер для защиты государства и граждан от нависшей криминальной угрозы. Задача правоохранительных органов состоит в организационном обеспечении их практической деятельности посредством осуществления стратегических и тактических мер нейтрализации противодействия криминальных элементов силам правопорядка.

Одним из направлений повышения результативности профессиональной деятельности сотрудников правоохранительных органов по предупреждению и пресечению криминальных действий, обеспечению эффективного функционирования силовых и властных структур является создание системы организации внедрения и комплексного использования достижений научно-технического прогресса, соблюдения требований обеспечения собственной безопасности и режима защиты информации. Использование современной специальной техники в значительной степени способствует оптимизации

управления деятельностью правоохранительных органов, и прежде всего по предупреждению и раскрытию преступлений, розыску преступников и лиц, похищенных или пропавших без вести, выявлению и пресечению разведывательной деятельности преступных сообществ, блокированию террористических актов, проведению оперативно-розыскных мероприятий. Технические средства позволяют не только получить и зафиксировать оперативно значимую информацию, но и обеспечить ее дальнейшую передачу по различным каналам связи в автоматизированный банк данных, осуществляя в рамках закона накопление необходимых сведений для последующей аналитической работы, в том числе по специальным компьютерным программам.

Важно отметить, что информация, полученная с использованием технических средств и систем и зафиксированная на материальном носителе, позволяет на стадии предварительного следствия или судебного разбирательства не только однозначно установить источник ее получения, но и убедительно доказать ее достоверность, обоснованность и объективность, а это немаловажно в процессе доказывания.

Достижения научно-технического прогресса при неукоснительном соблюдении законности во многом способствуют успешной работе правоохранительных органов.

Лекция 1. СПЕЦИАЛЬНАЯ ТЕХНИКА В СИСТЕМЕ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

1. Научно-технический прогресс и его влияние на правоохранительную деятельность.

2. Понятие, классификация и функции специальной техники в системе технического обеспечения правоохранительной деятельности.

3. Факторы, влияющие на эффективность применения специальной техники в правоохранительной деятельности.

1. Научно-технический прогресс и его влияние на правоохранительную деятельность

В современных условиях мощнейшего воздействия достижений научно-технического прогресса на все сферы общественной жизни, в том числе на правоприменительную деятельность, эффективность функционирования правоохранительной системы по решению возложенных на нее задач наряду с другими факторами во многом может быть обеспечена рациональным,

продуманным в правовом и организационном аспекте использованием технического потенциала.

Научно-технический прогресс представляет собой не только локальное явление, замкнутое рамками науки и техники. Это глобальный и универсальный процесс, протекающий в масштабах общества в целом, затрагивающий все стороны его развития. Причем усиление социальной ориентации научно-технического прогресса следует рассматривать в качестве одной из его главных закономерностей.

В свою очередь, нормы права должны охватывать все процессы и отношения, вытекающие из научно-технического прогресса.

В настоящее время научно-технические средства, разработанные на базе новейших достижений естественных и технических наук, внедренные в практику правоохранительных органов, оптимизируют их деятельность. Без использования на практике достижений научно-технического прогресса едва ли можно говорить об оптимальном обеспечении правопорядка.

Эффективность борьбы с преступностью и другие факторы находятся в прямой зависимости от используемых при этом средств и методов. Заметим, что чем в большей мере эти средства и методы основаны на новейших достижениях научно-технического прогресса, тем точнее и быстрее решаются задачи предупреждения и раскрытия преступлений. Следовательно, широкое использование результатов и достижений научно-технического прогресса является одним из важнейших направлений совершенствования правоохранительной деятельности.

Научно-технический прогресс непосредственно влияет на техническое обеспечение борьбы с преступностью: разрабатываемая и изготавливаемая для решения этих задач аппаратура, созданная на основе последних достижений электроники, становится все более надежной, эргономичной.

В общем виде результаты воздействия научно-технического прогресса на правоохранительную деятельность проявляются, по меньшей мере, в следующем:

- расширяются функции, выполняемые техническими средствами в процессе обеспечения правопорядка;
- совершенствуются виды и качество производимых технических средств, приемы их использования;
- появляются технические средства, способные эффективно обрабатывать большие объемы информации и выдавать за минимальное время результат этой обработки;
- сокращается количество персонала, обслуживающего комплексы технических средств.

В связи с повышением общего уровня научно-технического развития общества увеличиваются потенциальные способности сотрудников

правоохранительных органов к использованию специальной техники в своей служебной деятельности.

2. Понятие, классификация и функции специальной техники в системе технического обеспечения правоохранительной деятельности

Выражение «специальная техника» включает в себя две составляющие. Обратившись к толковым словарям русского языка, можно выяснить, что термин «специальная» означает особенная, исключительно для чего-либо предназначенная, а также относящаяся к отдельной отрасли чего-нибудь, присущая какой-нибудь специальности.

Под термином «техника» понимается, во-первых, совокупность средств труда, орудий, с помощью которых создают что-нибудь, во-вторых, непосредственно сами машины, орудия, устройства и, в-третьих, совокупность знаний, средств, способов, приемов, используемых в каком-либо деле.

Таким образом, техника, с одной стороны, – это совокупность средств деятельности, создаваемых для осуществления процессов производства и обслуживания непроеизводственных потребностей общества; с другой – совокупная характеристика используемых для достижения цели навыков и приемов (греческое слово «*techné*» означает мастерство).

Рассматривая вопрос несколько шире, отметим, что в настоящее время в системе технического обеспечения правоохранительной деятельности, помимо специальной техники, можно выделить технику управления, а также криминалистическую технику. При этом в состав техники управления, криминалистической и специальной техники может включаться определенный набор (на первый взгляд, иногда схожих) технических средств. Вместе с тем следует иметь в виду, что методы, приемы их применения и соответственно решаемые с их помощью частные задачи различны, во многом обусловлены той сферой деятельности, в которой применяются технические средства.

Так, с помощью техники управления обеспечивается, облегчается выполнение управленческих (организационных) задач. К техническим средствам управления можно отнести организационную технику, средства связи и передачи данных, автоматизированные системы обработки информации и управления.

В свою очередь, организационная техника включает в себя технические средства для составления и изготовления документов (например, портативные печатные машины, диктофоны), размножения документов (ксерокс), обработки документов (устройства для вскрытия конвертов, бумагоуничтожающие машины, ламинаторы и пр.), хранения документов (специальные шкафы для

подвесного хранения документов в папках, механизированные картотеки), для наглядного отображения информации (световые табло, диапроекторы, видеомониторы и пр.).

Другая разновидность техники управления – техника связи. Связь является основным средством, обеспечивающим управление в правоохранительных органах.

Использование автоматизированных (компьютеризированных) систем, а также средств связи и передачи данных в настоящее время направлено на информатизацию управления, которая преследует такие цели, как: повышение научной обоснованности и качества принимаемых решений благодаря использованию математических методов и моделей; гибкости управления и его способность реагировать на изменения условий деятельности исправительных учреждений; оперативности управления за счет своевременной и целенаправленной подготовки информации для принятия управленческих решений; производительности труда лиц, принимающих решения; снижение затрат на управленческую деятельность.

Специальную и криминалистическую технику следует отнести к разряду специфических средств, предназначенных для предупреждения и раскрытия преступлений.

Можно утверждать, что специальная техника «выросла» из криминалистической (на ранних этапах своего развития – «уголовной») техники, средства и методы которой перерабатывались с учетом их использования в охране общественного порядка, уголовно-исполнительной, административной и оперативно-розыскной деятельности.

В теории криминалистики криминалистическая техника рассматривается как система научных положений и разрабатываемых на их основе технических средств, приемов и методик, предназначенных для собирания, исследования и использования доказательств в процессе расследования преступлений. При этом в качестве технико-криминалистического средства может выступать любой предмет, если он отвечает установленным уголовно-процессуальным законом условиям использования для собирания и исследования доказательств.

В настоящее время криминалистическая техника подразделяется на следующие отдельные отрасли: криминалистическая фотография, видеосъемка; криминалистическая звукозапись; криминалистическое исследование документов; криминалистическое исследование оружия и следов его применения; трасология; судебная баллистика; габитоскопия (отождествление личности по внешним признакам); криминалистическая регистрация; криминалистическая одорология; криминалистическая фоноскопия.

С помощью технико-криминалистических средств и методов решаются задачи, связанные: с обнаружением, фиксацией, изъятием различных следов и иных объектов; накоплением, обработкой и использованием криминалистически значимой информации, содержащейся в следах преступлений; предварительным

и экспертным исследованием различных объектов, в том числе вещественных доказательств; научной организацией труда следователей, экспертов, судей.

Следовательно, технические средства являются криминалистическими в том случае, если они адаптированы, методически приспособлены к условиям деятельности по раскрытию и расследованию преступлений.

Что же, в свою очередь, вкладывается в понятие специальной техники, каково ее назначение в системе технического обеспечения правоохранительной деятельности?

Выражение «специальная техника» в узком смысле изначально ассоциируется с собственно специальными техническими средствами (приборами, устройствами, приспособлениями).

Однако в широком смысле это понятие должно учитывать двоякий подход к слову «техника» (с одной стороны, это средства, устройства, с другой – умения, навыки, приемы). При этом технические средства являются одной из составляющих более объемного понятия «специальная техника». Эти два термина соотносятся друг с другом как часть и целое, поскольку определение специальной техники будет неполным, если его ограничить лишь одними специальными техническими средствами. Заметим, что существуют еще и специальные приемы использования этих технических средств, применяемые уполномоченными на то субъектами, что тоже можно охарактеризовать как специальную технику (в контексте определенных умений, навыков и т. п.).

Таким образом, при определении понятия «специальная техника» следует исходить из того, что оно включает в себя не только собственно технические средства¹, различные приборы и приспособления, но и определенные (специальные) знания, способы, приемы их эффективного применения. Анализ научной литературы показывает, что такой подход лежит в основе подавляющего большинства существующих определений специальной техники.

Важная особенность состоит и в том, что специальная техника включает в себя технические средства и приемы их использования именно в борьбе с преступностью (правонарушениями). Естественно, что такое применение технических средств должно быть жестко регламентировано законом.

Итак, в широком понимании *специальная техника представляет собой совокупность технических средств и научно обоснованных приемов их правомерного использования уполномоченными на то сотрудниками правоохранительных органов в целях предупреждения и раскрытия преступлений, иных правонарушений, розыска преступников, содержания под стражей осужденных, а также лиц, подозреваемых и обвиняемых в совершении преступлений.*

В таком определении специальной техники обозначены следующие важные моменты:

- технические средства используются на основе соответствующих тактико-технических приемов, без которых они (технические средства) превращаются в никому не нужные устройства, приборы, приспособления и т. п. Причем как сама разработка технических средств, так и указанные приемы и рекомендации должны опираться на научные исследования и разработки, то есть иметь научную основу;

- субъекты применения технических средств – это прежде всего сотрудники правоохранительных органов;

- важнейшее условие применения специальной техники – правомерность ее использования в правоохранительной деятельности.

Следует иметь в виду, что в качестве одной из составляющих понятия «специальная техника» нужно рассматривать только те технические средства, которые либо специально изготовлены, либо приспособлены для решения задач обеспечения правопорядка, борьбы с преступностью и иными правонарушениями.

Специальная техника может быть общего и оперативно-розыскного назначения.

Специальная техника общего назначения применяется правоохранительными органами в процессе охраны общественного порядка и обеспечения общественной безопасности, административной деятельности, а также в сфере исполнения уголовных наказаний.

В качестве технических средств общего назначения можно рассматривать, например, средства связи, сигнализации, поисковые приборы и средства наблюдения, аппаратуру фото- и видеосъемки, звукозаписи и иные технические средства, как правило, бытовые (универсальные).

По своему конструктивному исполнению технические средства общего назначения изначально не приспособлены и не предназначены для решения задач оперативно-розыскной деятельности. Их использование носит открытый, гласный характер.

Специальная техника оперативно-розыскного назначения представляет собой совокупность технических средств и научно обоснованных специальных приемов их правомерного применения оперативными аппаратами в процессе осуществления оперативно-розыскных мероприятий. Эта техника применяется в сфере оперативно-розыскной деятельности оперативными работниками или другими лицами по их указанию, как правило, негласно, в целях решения задач, возложенных на оперативно-розыскную деятельность и определенных законом.

В качестве технических средств в процессе осуществления оперативно-розыскной деятельности используются те, которые специально созданы (приспособлены, запрограммированы) для негласного получения информации. К их числу нужно отнести следующие специальные технические средства, предназначенные:

- для негласного получения и регистрации акустической информации;

- негласного визуального наблюдения и документирования;
- негласного прослушивания телефонных переговоров;
- негласного перехвата и регистрации информации с технических каналов связи;
- негласного контроля почтовых сообщений и отправлений;
- негласного исследования предметов и документов;
- негласного проникновения и обследования помещений, транспортных средств и других объектов;
- негласного контроля за перемещением транспортных средств и других объектов;
- негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи;
- негласной идентификации личности.

Таким образом, специальная техника – это мощнейшее средство, позволяющее выявлять и документировать всевозможные факты противоправной деятельности и причастных к ней лиц, определенным образом фиксировать различные предметы, документы и следы, которые могут быть использованы в административной, уголовно-исполнительной, оперативно-розыскной и процессуальной деятельности правоохранительных органов.

Разграничение специальной техники на две рассмотренные группы (общего и оперативно-розыскного назначения) обусловлено, во-первых, сферой деятельности, в которой применяется специальная техника (например, административная и оперативно-розыскная); во-вторых, правовыми основаниями применения рассматриваемых технических средств в различных сферах правоохранительной деятельности; в-третьих, научной обоснованностью применения технических средств общего и оперативно-розыскного назначения, проверкой практикой эффективности и безопасности данных средств.

В зависимости от конструкции, исполнения и условий применения все технические средства, стоящие на вооружении правоохранительных органов, можно разделить на следующие виды:

- изготовленные специально для правоохранительных органов, являющиеся в полном смысле слова специальными техническими средствами (например, предназначенные для охраны объектов, поиска запрещенных металлических предметов, негласного получения информации);
- общего назначения (универсальные, бытовые), приспособленные для использования в специфических условиях деятельности правоохранительных органов;
- общего назначения (универсальные, бытовые), применяемые в исправительных учреждениях без переделки или приспособления.

Термин «специальный» может быть, с одной стороны, применен к совокупности технических средств, специально изготавливаемых для правоохранительных органов, приспособляемых в специфических условиях

для решения задач обеспечения правопорядка, с другой – и к особым приемам (способам, методам) использования технических средств в правоохранительной деятельности.

Так, персональный компьютер (ПК) облегчает составление и распечатку различных документов и представляет собой средство организационной техники. Однако он становится средством специальной техники, если, например, выступает как устройство, способное посредством специальной программы выдать правильную рекомендацию сотруднику правоохранительных органов при раскрытии какого-либо правонарушения, то есть проанализировать сложившуюся ситуацию и выдать верный алгоритм действий, как правило, в условиях дефицита времени.

Подобный подход применяется и к служебному транспорту, используемому в правоохранительных органах. Сам по себе автомобиль (автобус, катер, вагон и т. д.) не является специальным техническим средством. Автомашину (иное транспортное средство) можно отнести к средствам специальной техники лишь после ее оборудования, доукомплектования специальными техническими средствами, предназначенными, например, для решения задачи изоляции осужденных при их конвоировании, этапировании. И тогда служебный автомобиль, оборудованный инженерно-техническими средствами охраны, будет представлять собой средство специальной техники для обеспечения выполнения функции охраны и конвоирования осужденных.

Необходимо отметить, что наряду с понятием специальной техники в литературе и на практике применяется ведомственный термин «специальные средства» для обозначения различных групп средств индивидуальной защиты, активной обороны, обеспечения проведения специальных операций. Причем существует тенденция относить специальные средства к одному из видов (групп, классов) специальной техники. Вопрос отнесения специальных средств в разряд либо специальной техники, либо в самостоятельный вид в настоящее время является дискуссионным, требующим научной проработки.

Вместе с тем можно заметить, что, хотя резиновые палки и наручники не относятся к собственно техническим средствам (приборам, аппаратам и т. п.), целью их применения является физическое воздействие на правонарушителя, пресечение его противоправных действий либо попыток их совершения. Водометы и бронемашины представляют собой специальные средства, относящиеся (учитывая направленность их применения – оказание физического и психологического воздействия на нарушителей порядка) к специальному вооружению и бронетехнике.

Светозвуковые средства отвлекающего воздействия имеют особую специальную цель – воздействие на органы чувств правонарушителя, для того чтобы временно вывести его из строя, дезориентировать, деморализовать путем светового ослепления, звукового оглушения. К тому же в определенном аспекте светозвуковые средства отвлекающего воздействия подпадают под понятие

«сигнальное оружие», то есть «оружие, конструктивно предназначенное только для подачи световых, дымовых или звуковых сигналов» (ст. 1 Федерального закона от 13 декабря 1996 г. «Об оружии»).

Средства разрушения преград, под которыми традиционно понимаются малогабаритные взрывные устройства типа «Ключ» и «Импульс», а также патроны с резиновой пулей, вышибные патроны к специальному карабину типа «КС-23» на основании Закона «Об оружии» следует отнести к боеприпасам, то есть к предметам вооружения и метаемому снаряжению, предназначенным для поражения цели и содержащим разрывной, метательный, пиротехнический или вышибной заряды либо их сочетание.

Изделие типа «Черемуха» или «Сирень» в различном исполнении (газовые гранаты, патроны, аэрозольные баллоны), а также газовые пистолеты и револьверы, карабин «КС-23» подпадают под определение Закона как газовое оружие, предназначенное для временного поражения живой цели путем применения слезоточивых или раздражающих веществ.

Таким образом, специальную технику и специальные средства (в узком, обозначенном нами смысле) целесообразно рассматривать как два отдельных самостоятельных средства обеспечения правопорядка. Если в определении первой из обозначенных нами категорий фигурируют отдельные технические средства, системы и комплексы, то во второй – преимущественно средства специального вооружения (газовое оружие, ударные и противоударные средства активной обороны, средства бронезащиты и т. п.), а также служебные собаки. Причем применение технических средств направлено в первую очередь на получение различного рода информации о факте либо возможности совершения правонарушения. А использование специальных средств предполагает определенное физическое воздействие на правонарушителя (слезоточивым газом, светом и звуком, ударом палкой, резиновой пулей и т. п.), место его укрытия (например, открывание двери посредством взрывных устройств) либо защиту сотрудников от предполагаемого нападения (каска, бронежилет, щит и т. д.).

Следовательно, непосредственные цели применения специальной техники и специальных средств (в нашем понимании этого термина) в процессе укрепления правопорядка различны. Поэтому специальные средства (индивидуальной защиты, активной обороны, обеспечения специальных операций) не являются каким-либо видом (разновидностью, подгруппой) специальной техники и не входят в ее классификацию.

Требования, предъявляемые к применению специальной техники, следующие: соблюдение законности, целесообразность, активность, наступательность. Кроме того, на применение специальной техники оперативно-розыскного назначения накладывается дополнительное требование – обеспечение конспирации.

Соблюдение законности применения специальной техники выражается в том, что использование каждого технического средства в правоохранительной деятельности должно строго соответствовать требованиям правовых норм.

Использование специальной техники должно быть направлено на обеспечение охраны общественного порядка и общественной безопасности, выявление, предупреждение и раскрытие преступлений и административных правонарушений, нарушений установленного порядка отбывания наказаний в местах лишения свободы, розыск преступников, лиц, уклоняющихся от отбывания наказания.

Кроме того, технические средства должны применяться в соответствии с нормами нравственности, быть безопасны для жизни и здоровья людей, не наносить вред окружающей среде. Важное значение имеет правильное документальное оформление применения специальной техники.

Целесообразность заключается в научной и практической обоснованности применения специальной техники в правоохранительной деятельности. Иными словами, в каждой конкретной ситуации должны использоваться такие технические средства и соответствующие приемы их применения, которые обеспечат наиболее эффективный результат.

Активность предполагает систематическое и комплексное применение специальной техники на основе предварительного планирования. Сотрудники правоохранительных органов должны иметь четкое представление о возможностях использования технических средств в обеспечении правопорядка.

Наступательность состоит в том, что технические средства должны применяться на основе прогнозирования противоправного поведения правонарушителя в то время и в том месте, которые наиболее целесообразны для решения конкретных служебных задач.

Обеспечение конспирации заключается в соблюдении режима секретности в отношении сведений о специальных технических средствах, разработанных, приспособленных, запрограммированных для негласного получения информации в ходе осуществления оперативно-розыскной деятельности (их конструкциях, тактико-технических данных, конкретном применении в оперативно-розыскных мероприятиях), об условиях, тактических приемах и субъектах их применения, а также сведений, полученных в результате использования такой техники.

Рассматривая в целом *функцию специальной техники* в правоохранительной деятельности, следует исходить из того, что специальная техника является лишь одним из компонентов сложной системы сил, средств и методов, предназначенных для предупреждения, пресечения и раскрытия криминальных деяний, административных правонарушений, нарушений установленными установленными порядка отбывания наказания. Поэтому целесообразнее говорить о вкладе специальной техники в выполнение задачи обеспечения правопорядка.

К непосредственной цели применения собственно технических средств следует отнести получение и обработку информации, представленной в различных вариантах, имеющей значение для предупреждения, пресечения и раскрытия правонарушений. Собираемая с помощью специальной техники информация, по сути, представляет собой содержание сообщения, сигнала, памяти, а также сведения, содержащиеся в сообщении, сигнале, памяти. С этой точки зрения можно говорить об информационной функции специальной техники, а точнее, о функции обеспечения сбора информации (сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления) для нужд поддержания правопорядка.

При этом информационно-предупредительное значение специальной техники состоит в том, что с ее помощью при определенных условиях можно получить сведения о противоправных замыслах, приготовлениях к преступным (противоправным) деяниям, а затем, имея такую информацию, принять меры по предотвращению (пресечению) противоправных действий. К тому же осведомленность лиц об использовании (возможности применения) в отношении их специальной техники, в свою очередь, является фактором, сдерживающим от совершения правонарушения.

Значение специальной техники в раскрытии правонарушений (в информационном аспекте) обусловлено тем, что посредством ее применения собирается информация об обстоятельствах совершенного противоправного деяния, а именно фактические данные (источники доказательств), представляющие собой признаки тех или иных противоправных действий, отраженные во внешней среде в различных формах.

Вместе с тем отдельные инженерно-технические средства за счет своего конструктивного исполнения обеспечивают разграничение территории, изоляцию лиц, содержащихся под стражей, создают преграду для совершения противоправных действий, помогают осуществлять функцию охраны и надзора.

Следовательно, специальная техника выполняет вспомогательную функцию в обеспечении правопорядка, решении задач, возложенных на ту сферу правоохранительной деятельности, в рамках которой она применяется.

3. Факторы, влияющие на эффективность применения специальной техники в правоохранительной деятельности

Фактор – это момент, существенное обстоятельство в каком-нибудь процессе, явлении. В нашем случае этот процесс (явление) представляет собой деятельность по применению специальной техники.

Термин «эффективность» часто объясняется как результативность, степень достижения цели. Однако, рассматривая эффективность применения специальной техники в обеспечении правопорядка, необходимо учитывать не только степень достижения цели использования технических средств, то есть

получение оптимальных (наилучших) результатов наиболее рациональным путем, но и затраты (материальные, временные, человеческой энергии и т. д.), произведенные для достижения цели. При таком подходе эффективность можно определить с помощью соотношения полученных результатов и вызванных ими затрат.

Вместе с тем эффективность специальной техники может определяться и с учетом того вклада, который она вносит в достижение целей правоохранительной деятельности, в обеспечение правопорядка.

К факторам, влияющим на эффективность использования специальной техники, можно отнести следующие: организационно-управленческий, технический, тактический, кадровый, правовой.

Организационно-управленческий фактор направлен на создание благоприятных условий для применения специальной техники в процессе деятельности по обеспечению правопорядка.

Следует отметить, что уровень организации деятельности по внедрению и использованию технических средств в правоохранительных органах во многом определяется руководителями (начальником учреждения, его заместителями, начальниками соответствующих структурных подразделений), которые обязаны:

- обеспечить структурные подразделения необходимыми техническими средствами в соответствии с нормами положенности;
- организовать правомерное применение специальной техники в целях обеспечения правопорядка;
- систематически осуществлять контроль за правильной эксплуатацией технических средств;
- обеспечить взаимодействие структурных подразделений по организации внедрения и эффективному применению специальной техники при обеспечении правопорядка;
- обеспечить внутреннее (в рамках своего подразделения) и внешнее (своего подразделения с другими подразделениями) взаимодействие в вопросах применения технических средств в борьбе с преступностью и иными правонарушениями;
- периодически анализировать состояние использования технических средств, выявлять и поощрять положительный опыт сотрудников по применению технических средств;
- организовать техническую подготовку и переподготовку персонала.

Технический фактор, влияющий на эффективность применения специальной техники, определяется следующими показателями:

- наличие необходимых технических средств, удовлетворяющих потребности правоохранительных органов;
- укомплектованность структурных подразделений средствами специальной техники в соответствии с нормами табельной положенности;

- техническая исправность средств специальной техники;
- надежность используемых технических средств.

Тактический фактор, влияющий на эффективность применения специальной техники, представляет собой оптимальную реализацию конкретных способов правомерного использования технических средств, тактико-технические характеристики которых в данный момент лучше всего обеспечивают достижение требуемой цели. Он определяется:

- конкретной ситуацией, возникающей в процессе обеспечения правопорядка, в которой применяется то или иное техническое средство;
- тактико-техническими характеристиками средств специальной техники, используемых в данной ситуации;
- методикой применения технического средства;
- положениями ведомственных нормативных документов, регламентирующих пределы правомерного применения специальной техники.

Кадровый фактор во многом влияет на эффективность применения специальной техники в правоохранительной деятельности. Очевидно, что при оснащении соответствующего структурного подразделения необходимым набором самых современных технических средств возникает вопрос о том, кто их будет применять. При отсутствии в подразделении сотрудников, владеющих приемами использования технических средств, разговор об эффективности применения специальной техники не имеет смысла.

Правовой фактор представляет собой оптимальность нормативно-правового регулирования деятельности по применению специальной техники в обеспечении правопорядка. Этот фактор определяется такими показателями, как:

- наличие законодательных норм, регламентирующих допустимость использования технических средств в обеспечении правопорядка;
- нормативная регламентация организации, тактики и методики применения отдельных видов специальной техники в различных сферах правоохранительной деятельности;
- нормативная регламентация использования результатов применения специальной техники в правоохранительной деятельности;
- нормативная регламентация технической эксплуатации специальной техники;
- нормативная регламентация обеспечения правоохранительных органов техническими средствами;
- нормативное закрепление квалификационных требований для сотрудников правоохранительных органов по освоению и применению технических средств в деятельности по обеспечению правопорядка.

Таким образом, эффективность применения специальной техники определяет комплекс показателей, относящихся к факторам организационно-управленческого, технического, тактического, кадрового и правового характера.

В целом организационно-управленческий фактор, влияющий на применение специальной техники, характеризуется деятельностью руководителей правоохранительных органов; технический фактор – наличием достаточного количества работоспособных и надежных технических средств, необходимых для обеспечения правопорядка; тактический фактор – способами оптимального использования специальной техники в различных ситуациях оперативно-служебной деятельности; кадровый фактор – наличием субъектов, способных применять специальную технику в деятельности по обеспечению правопорядка; правовой фактор – наличием правовых (юридических) норм, регламентирующих все аспекты деятельности, связанные с применением специальной техники в правоохранительной деятельности.

Лекция 2. ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ПРИМЕНЕНИЯ СПЕЦИАЛЬНОЙ ТЕХНИКИ

- 1. Система правового регулирования применения специальной техники.*
- 2. Организационные основы применения специальной техники.*

1. Система правового регулирования применения специальной техники

Возрастающая роль технических средств в деятельности правоохранительных органов, накопленный положительный опыт по их применению создают предпосылки для научного осмысления и совершенствования правовой основы применения специальной техники в обеспечении правопорядка. Актуальность данной проблемы определяется тем, что уровень разработки правового аспекта применения технических средств во многом обуславливает эффективность использования специальной техники в правоохранительной деятельности.

Правовая основа применения специальной техники – это система законодательных и подзаконных актов, а также устанавливаемых ими принципов и правил, определяющих допустимость использования либо регламентирующих организацию, порядок, условия, способы и результаты использования технических средств в обеспечении правопорядка.

Нормативно-правовое регулирование применения специальной техники в правоохранительной деятельности включает в себя:

- нормы Конституции Российской Федерации;
- нормы законов Российской Федерации;
- нормативно-правовые акты Президента и Правительства РФ;
- межведомственные нормативно-правовые акты;

- ведомственные нормативные акты.

Законодательной основой правового регулирования применения специальной техники является Конституция Российской Федерации – основа всего федерального законодательства, ее нормы имеют прямое действие.

Конституция Российской Федерации содержит основные предписания по вопросам безопасности, обеспечения прав и свобод граждан, охраны собственности и общественного порядка.

Согласно Конституции РФ человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина являются обязанностью государства (ст. 2). Поэтому в процессе применения технических средств в правоохранительной деятельности следует неукоснительно выполнять требования норм Конституции РФ, которые закрепляют право граждан на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23). Ограничение этого права допускается только на основании судебного решения.

Не допускается распространение информации о частной жизни лица (равно как и сбор, хранение, использование сведений) без его согласия (п. 1 ст. 24). Согласно Конституции РФ (ст. 25) жилище неприкосновенно, что означает недопустимость не только вхождения в него против воли проживающих, но и незаконного использования различных технических средств для прослушивания разговоров в жилище, видеоконтроля обстановки и т. п.

Вместе с тем Конституция РФ предоставляет правоохранительным органам, другим структурам обеспечения государственной безопасности существенные возможности по сбору, накоплению, обработке и использованию информации (ст. 55). Следовательно, применение правоохранительными органами технических средств возможно не только для получения в рамках закона необходимой информации, но и защиты на законных основаниях информационных и имущественных прав и свобод граждан.

В Российской Федерации приняты и действуют законодательные акты, которые содержат нормы, допускающие использование технических средств и соответствующих приемов и действий в процессе осуществления правоохранительной деятельности.

Так, *Закон Российской Федерации «О милиции»* обязывает органы милиции (ст. 10) принимать и регистрировать заявления, сообщения и иную поступающую информацию о преступлениях, административных правонарушениях и событиях, угрожающих личной или общественной безопасности. Прием и регистрация поступающей информации могут осуществляться с использованием технических средств и информационных технологий.

Согласно Закону милиция обязана проводить экспертизу по уголовным делам, а также научно-технические исследования по материалам оперативно-розыскной деятельности.

Закон предоставляет милиции право (ст. 11) осуществлять предусмотренные законодательством учеты физических и юридических лиц, предметов и фактов и использовать данные этих учетов; применять для документирования своей деятельности информационные системы, видео- и аудиотехнику, кино- и фотоаппаратуру, а также другие технические и специальные средства, не причиняющие вреда жизни, здоровью человека и окружающей среде.

Кроме того, милиция имеет право производить регистрацию, фотографирование, звукозапись, кино- и видеосъемку, дактилоскопирование лиц, заключенных под стражу, задержанных по подозрению в совершении преступления или занятии бродяжничеством, обвиняемых в совершении преступлений, подвергнутых административному аресту, а также лиц, подозреваемых в совершении административного правонарушения при невозможности установления их личности и иных лиц в соответствии с законодательством Российской Федерации.

Милиция имеет право осуществлять оперативно-розыскную деятельность в соответствии с федеральным законом.

Закон Российской Федерации от 21 июля 1993 г. «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» предоставляет учреждениям УИС право (ст. 14) осуществлять в соответствии с законодательством Российской Федерации оперативно-розыскную деятельность, а также наряду с другими правами осуществлять регистрацию осужденных, их фотографирование, звукозапись, кино- и видеосъемку и дактилоскопирование.

Федеральный закон от 12 августа 1995 г. «Об оперативно-розыскной деятельности» – базовый акт в вопросах применения специальной техники оперативно-розыскного назначения – разрешает оперативным аппаратам правоохранительных органов – субъектов ОРД использовать в ходе проведения оперативно-розыскных мероприятий информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и вреда окружающей среде (ст. 6).

Статья 6 Федерального закона «Об оперативно-розыскной деятельности» позволяет использовать для решения задач оперативно-розыскной деятельности помощь специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе, но в то же время запрещает использование специальных и иных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, не уполномоченными на то данным Законом физическими и

юридическими лицами. Перечень специальных технических средств, предназначенных для негласного получения информации, устанавливается Правительством Российской Федерации.

Федеральный закон «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений» (принят Государственной Думой 21 июня 1995 г.) в ст. 34 указывает, что в целях осуществления надзора за подозреваемыми и обвиняемыми может использоваться аудио- и видеотехника. Кроме того, заключенные подвергаются личному обыску, дактилоскопированию и фотографированию, помещения, в которых они размещаются, – обыску, а их вещи и посылки – досмотру. В местах содержания под стражей в целях выявления, предупреждения, пресечения и раскрытия преступлений проводятся оперативно-розыскные мероприятия.

Уголовно-исполнительный кодекс РФ регламентирует применение технических средств в исправительных учреждениях. Статья 83 УИК РФ «Технические средства надзора и контроля» предоставляет администрации исправительных учреждений право использовать аудиовизуальные, электронные и иные технические средства надзора и контроля для предупреждения побегов и других преступлений, нарушений установленного порядка отбывания наказания и в целях получения необходимой информации о поведении осужденных. Вместе с тем администрация исправительных учреждений обязана под расписку уведомлять осужденных о применении указанных средств надзора и контроля (ч. 2 ст. 83 УИК РФ). Перечень и порядок использования указанных технических средств устанавливаются нормативными правовыми актами Российской Федерации (ч. 3 ст. 83 УИК РФ).

Заметим, что УИК РФ в ст. 84 регламентирует оперативно-розыскную деятельность, осуществляемую в исправительных учреждениях. В связи с этим оперативные аппараты УИС вправе использовать все методы и средства ОРД, включая применение специальной техники оперативно-розыскного назначения.

Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. содержит нормы, в которых подразумевается допустимость либо указана возможность использования технических средств, а также полученных с их помощью результатов в уголовном судопроизводстве (досудебном и судебном разбирательстве по уголовному делу).

Использование технических средств при производстве следственных действий во многом способствует получению достоверных и обоснованных доказательств. При этом в протоколе следственного действия должны быть указаны технические средства, примененные в следственном действии, а также условия и порядок их использования, объекты, к которым эти средства были применены, и полученные результаты. Обязательным условием (с отражением в протоколе) является предупреждение лиц, участвующих в следственном действии, о применении технических средств.

УПК РФ предусматривает участие специалиста, который, используя свои специальные знания и навыки, будет оказывать помощь в обнаружении, закреплении и изъятии доказательств с помощью технических средств.

Следует заметить, что применение специальной техники представляет собой, по существу, информационный процесс, в котором технические средства выступают в качестве средств сбора и выдачи информации. Современные технические средства становятся все более компьютеризированными.

Задача законодательного урегулирования информационных процессов, возникающих при использовании технических средств и информационных технологий, во многом решается *Федеральным законом от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»*. Он регламентирует информационные отношения, возникающие при формировании информационных ресурсов, создании и использовании информационных технологий и средств их обеспечения, а также при защите информации и прав субъектов, участвующих в информационных процессах.

Закон Российской Федерации от 21 июля 1993 г. «О государственной тайне» определил средства защиты информации как «технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации» (ст. 2).

Рассматриваемый Закон отнес к государственной тайне сведения «о силах, средствах, источниках, методах, планах и результатах» оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, «если они раскрывают перечисленные сведения» (п. 4 ст. 5). Процесс применения специальной техники оперативно-розыскного назначения при проведении оперативно-розыскных мероприятий, используемые при этом силы, средства, полученные фактические результаты регулируются и этой законодательной нормой.

Федеральный закон от 7 июля 2003 г. «О связи» установил правовую основу деятельности в области связи, осуществляемой под юрисдикцией Российской Федерации, определил полномочия органов государственной власти по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи. Законом определяются основные положения о связи в Российской Федерации.

Отметим, что средства связи – это технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправок, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи. Настоящий Федеральный закон (ст. 2) определяет основные термины, относящиеся к деятельности в

области связи, такие как «электросвязь», «сеть связи», «средства связи», «пользователи услуг связи» и др.

Статья 12 указывает, что единая сеть электросвязи Российской Федерации состоит из расположенных на территории Российской Федерации сетей электросвязи следующих категорий:

- сеть связи общего пользования;
- выделенные сети связи;
- технологические сети связи, присоединенные к сети связи общего пользования;
- сети связи специального назначения и другие сети связи для передачи информации при помощи электромагнитных систем.

Так, выделенными сетями связи являются (ст. 14) сети электросвязи, предназначенные для возмездного оказания услуг электросвязи ограниченному кругу пользователей или группам таких пользователей. Выделенные сети связи могут взаимодействовать между собой. Они не имеют присоединения к сети связи общего пользования, а также к сетям связи общего пользования иностранных государств. Технологии и средства связи, применяемые для организации выделенных сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей.

Выделенная сеть связи может быть присоединена к сети связи общего пользования с переводом в категорию сети связи общего пользования, если выделенная сеть связи соответствует требованиям, установленным для сети связи общего пользования. При этом выделенный ресурс нумерации изымается и предоставляется ресурс нумерации из ресурса нумерации сети связи общего пользования.

Статья 16 посвящена сетям связи специального назначения, которые предназначены для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Следует отметить, что на физических и юридических лиц налагается юридическая ответственность за незаконное использование специальных и иных технических средств, предназначенных для негласного получения информации.

В соответствии с ч. 1 ст. 138 *Уголовного кодекса РФ* нарушение тайны переписки, телефонных переговоров, почтовых и иных сообщений наказывается штрафом в размере от 80 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от 120 до 180 часов, либо исправительными работами на срок до одного года. При этом объективная сторона преступления выражается как в незаконном ознакомлении с содержанием телефонных переговоров и почтово-телеграфной корреспонденции, так и в придании огласке сообщенных гражданами друг другу сведений.

Часть 2 ст. 138 УК РФ предусматривает наказание за то же деяние, совершенное лицом с использованием своего служебного положения или

специальных технических средств, предназначенных для негласного получения информации. При этом наказанием может быть штраф в размере от 100 тыс. до 300 тыс. руб. или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок от 180 до 240 часов, арестом на срок от двух до четырех месяцев.

В части 3 ст. 138 УК РФ предусматривается ответственность за незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации. Наказанием может быть штраф в размере от 200 тыс. до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Кроме того, самовольное и несанкционированное использование специальных технических средств, предназначенных для негласного получения информации, может быть квалифицировано как превышение власти или служебных полномочий. При этом ответственность определена в ст. 203 УК РФ «Превышение полномочий служащими частных охранных или детективных служб», а также в соответствии со ст. 286 «Превышение должностных полномочий».

Кодекс Российской Федерации об административных правонарушениях от 31 декабря 2001 г., с одной стороны, устанавливает административную ответственность (штраф в различных размерах минимальной оплаты труда) за неправомерные действия, связанные с проектированием, изготовлением, реализацией, установкой, эксплуатацией радиоэлектронных средств и высокочастотных устройств и иным оборудованием, функционирующим на основе законов электроники и радиотехники (ст. 13.3, 13.4, 13.8), а также оборотом и использованием специальных технических средств, предназначенных для негласного получения информации (ст. 20.23, 23.24). С другой стороны, Кодекс закрепляет возможность использования различных технических средств в административной деятельности, при производстве по делу об административном правонарушении (ст. 26.5, 27.7–27.10, 27.14) с отражением соответствующей информации в протоколе.

В производстве по делу об административном правонарушении возможно участие специалиста (ст. 25.8) и эксперта (ст. 25.9), обладающих необходимыми познаниями в технике и применении технических средств.

Доказательством по делу об административном правонарушении могут быть фактические данные, в том числе устанавливаемые показаниями специальных технических средств (ст. 26.2). К документам, признанным в качестве доказательств, могут быть отнесены материалы фото- и киносъемки, звуко- и

видеозаписи, информационных баз и банков данных и иные носители информации (ст. 26.7). Показания специальных технических средств, утвержденных в установленном порядке в качестве средств измерения, имеющих соответствующие сертификаты и прошедших метрологическую проверку, отражаются в протоколе об административном правонарушении (ст. 26.8).

Законодательные нормы, определяющие общие основания применения специальной техники, являются исходными для подзаконных нормативных актов, непосредственно регламентирующих использование технических средств в обеспечении правопорядка.

В настоящее время Президентом Российской Федерации приняты и действуют указы, в той или иной мере регламентирующие правоотношения в области применения технических средств в правоохранительной деятельности. В частности, Указом Президента РФ от 9 января 1996 г. № 21 перед органами Федеральной службы безопасности России поставлены следующие задачи:

- координация деятельности оперативных подразделений субъектов оперативно-розыскной деятельности с целью выявления нарушений правил разработки, производства и реализации специальных технических средств, предназначенных для негласного получения информации;

- выявление и пресечение фактов неправомерного использования таких средств;

- лицензирование деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации.

Нормативные акты Правительства Российской Федерации также входят в систему правового регулирования применения специальной техники. Так, например, Постановлением Правительства РФ от 1 июля 1996 г. № 770 в соответствии с Федеральным законом «Об оперативно-розыскной деятельности» утвержден перечень видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности.

Следующую группу нормативно-правовых документов, регулирующих применение специальной техники в правоохранительной деятельности, составляют межведомственные и ведомственные нормативные правовые акты.

В отдельную группу таких документов входят ведомственные нормативные акты по вопросам технической политики различных правоохранительных органов, в частности органов внутренних дел, акты, утверждающие перечень новых образцов технических средств, принятых на их вооружение, а также нормативные документы, регламентирующие нормы табельной положенности

подразделений правоохранительных органов техническими средствами, сроки их эксплуатации.

Из совокупности ведомственных нормативно-правовых актов, регулирующих применение специальной техники в правоохранительной деятельности, следует выделить те, которые регламентируют использование технических средств общего назначения и специальной техники оперативно-розыскного назначения.

Первые, как правило, являются ведомственными нормативно-правовыми актами открытого (несекретного) характера, вторые – закрытого (секретного, служебного) характера.

Так, в настоящее время в систему правового регулирования применения специальной техники общего назначения в уголовно-исполнительной системе (УИС) входят следующие ведомственные нормативно-правовые акты, принятые и утвержденные Министерством юстиции Российской Федерации и Федеральной службой исполнения наказаний, посвященные вопросам:

- оборудования инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы;
- технической эксплуатации инженерно-технических средств охраны и надзора в учреждениях УИС;
- организации связи в уголовно-исполнительной системе.

Эти ведомственные акты непосредственным образом регламентируют аспекты, касающиеся организации применения и эксплуатации инженерно-технических средств охраны, надзора и связи в учреждениях, исполняющих наказания.

Кроме того, нормы, разрешающие использование технических средств, определяющие условия их применения в учреждениях УИС, можно встретить, например, в Правилах внутреннего распорядка следственных изоляторов уголовно-исполнительной системы, Инструкции по охране исправительных учреждений, следственных изоляторов уголовно-исполнительной системы, Инструкции о надзоре за осужденными, содержащимися в исправительных колониях и других подобных нормативно-правовых актах.

Переходя к рассмотрению ведомственных нормативных правовых актов, регулирующих применение технических средств в оперативно-розыскной деятельности, отметим следующее.

Во-первых, применение специальной техники оперативно-розыскного назначения неотделимо от оперативно-розыскной деятельности, в связи с чем нормы, ее регулирующие, должны соответствовать иным нормативным актам, действующим в сфере оперативно-розыскной деятельности.

Во-вторых, законодательные нормы, определяющие общие основания (допустимость) применения технических средств в оперативно-розыскной деятельности, являются исходными для подзаконных нормативных актов, непосредственно регламентирующих использование конкретных видов специальных технических средств.

В-третьих, ведомственные нормативно-правовые акты, регламентирующие использование технических средств в оперативно-розыскной деятельности, а также организацию и тактику функционирования специализированных оперативно-технических подразделений, относятся к закрытым документам.

Среди ведомственной нормативно-правовой базы применения специальной техники можно выделить акты, содержащие наиболее общие положения по применению технических средств и соответствующих приемов действий с ними, а также нормы, относящиеся к конкретным видам технических средств.

2. Организационные основы применения специальной техники

Наличие лишь одних правовых оснований использования технических средств в правоохранительной деятельности без четкой организации процесса их применения не сможет обеспечить эффективность работы специальной техники.

Организация применения специальной техники в общем виде направлена на создание оптимальных условий для осуществления технического обеспечения тех или иных мероприятий по поддержанию правопорядка.

Организация как функция управления в сфере применения специальной техники – это вид управленческой деятельности, осуществляемой в правоохранительных органах, который представляет собой разработку и осуществление конкретных мер, связанных:

- с подбором исполнителей и доведением до них задач;
- выбором приоритета задач, способа и срока их решения;
- маневрированием имеющимися ресурсами;
- контролем;
- взаимодействием.

Эти меры направлены на оптимальную реализацию принятого решения по использованию технических и соответствующих тактико-технических приемов в обеспечении правопорядка.

Назначение организации применения специальной техники состоит в том, чтобы сформировать в правоохранительной системе такие организационные отношения, которые могли бы обеспечить правопорядок с минимальными затратами сил и средств.

В правоохранительных органах существуют определенные структуры, подразделения, в функции которых входят организация и качественное применение специальной техники. Так, в уголовно-исполнительной системе функционируют подразделения инженерно-технического и оперативно-технического обеспечения.

Такие организационно-функциональные структуры являются многоуровневыми. Например, в сфере организации использования специальной

техники общего назначения можно выделить систему инженерно-технического обеспечения (ИТО) служебной деятельности учреждений УИС, в состав которой входят:

- на уровне ФСИН России – Управление ИТО и вооружения, отдел ИТО, отдел связи, Главный центр инженерно-технического обеспечения (ГЦИТО);
- на уровне территориального органа УИС (ГУФСИН, УФСИН) – управление, отдел (отделение) ИТО, связи и вооружения, ЦИТО;
- на уровне исправительного учреждения и следственного изолятора – группа инженерно-технического обеспечения и связи.

Рассматривая организационные вопросы в сфере специальной техники, необходимо разграничивать такие категории, как «субъект применения» и «субъект организации применения» технических средств и соответствующих тактико-технических приемов в обеспечении правопорядка.

Субъекты применения специальной техники – это в широком смысле отдельные структурные подразделения, а в узком – сотрудники правоохранительных органов и иные лица (например, гражданские лица, обладающие необходимыми познаниями), непосредственно применяющие технические средства при выполнении задач обеспечения правопорядка.

Среди субъектов применения различных видов технических средств следует различать:

- специалистов, для которых эксплуатация технических средств является непосредственным содержанием их функциональных обязанностей. Такими специалистами, например, являются сотрудники специализированных инженерно-технических и оперативно-технических подразделений, отдельные специалисты по применению технических средств, инженеры по специальной технике;
- неспециалистов – сотрудников правоохранительных органов, использующих специальную технику для повышения эффективности осуществления профессиональной деятельности.

К *субъектам организации (организаторам)* применения специальной техники в правоохранительных органах следует относить соответствующих руководителей, начальников структурных подразделений, в той или иной мере отвечающих за организацию использования технических средств в обеспечении правопорядка.

При выполнении своих функциональных обязанностей субъекты организации применения специальной техники в правоохранительных органах, в пределах своей компетенции, организуют:

- техническую эксплуатацию средств специальной техники;
- непосредственное применение специальной техники в обеспечении правопорядка;
- изучение и внедрение передового опыта применения специальной техники;

- техническую подготовку (обучение, переподготовку) подчиненных сотрудников.

Основные функциональные обязанности, накладываемые на сотрудников правоохранительных органов (не специалистов по применению технических средств) в плане применения специальной техники, заключаются в следующем:

- знание правовых основ применения специальной техники;
- знание наименований, основных технических характеристик используемых технических средств;
- бережное отношение к технике, использование технических средств по прямому назначению;
- знание основ эксплуатации используемых средств специальной техники, то есть данные сотрудники должны иметь навыки работы с приборами и устройствами, применяемыми в правоохранительной деятельности.

Кроме того, каждый, кто использует названные технические средства, обязан знать и соблюдать правила ведения переговоров, основы дисциплины связи.

Лекция 3. СРЕДСТВА СИСТЕМЫ ЗАЩИТЫ ОБЪЕКТОВ

- 1. Структура комплексной защиты объектов.**
- 2. Системы и средства охранно-пожарной сигнализации.**
- 3. Системы и средства защиты объектов уголовно-исполнительной системы.**

1. Структура комплексной защиты объектов

Система комплексной защиты объектов – это совокупность технических и инженерных средств, а также соответствующих тактических приемов и методов их применения, направленных на обеспечение установленного порядка на обслуживаемой территории. Эти системы можно условно разделить на две группы: 1) системы и средства контроля и управления доступом, 2) системы и средства противопожарной защиты объектов, к которым относятся:

- система управления и контроля доступа;
- система охранной сигнализации;
- система пожарной сигнализации;
- система видеонаблюдения;
- система защиты информации;
- система жизнеобеспечения;
- персонал службы безопасности;
- спецсредства досмотра, отражения и ликвидации угроз;
- процедурные средства;

- система оперативной и громкоговорящей связи;
- элементы строительных конструкций;
- инженерные средства защиты.

Система управления и контроля доступа (СКУД) на объекте предназначена для исключения несанкционированного доступа персонала и посетителей на территорию, локальные охраняемые участки, в его режимные категорированные помещения, а также для предупреждения злоумышленных нарушений персоналом установленного порядка работы в особо важных зонах и предотвращения хищений товарно-материальных ценностей посетителями в рабочее время.

В центральном управляющем компьютере (сервере) системы архивируется вся информация не только о перемещениях персонала через границы охраняемых зон, но и о состоянии других систем защиты объекта, что позволяет дежурному оператору сервера оценивать оперативную обстановку, выявлять угрозы и управлять системой комплексной защиты объекта.

Система охранной сигнализации предназначена для обнаружения в период охраны попыток проникновения или совершения краж материальных ценностей, сбора, обработки, передачи и представления информации с системы управления и контроля доступа. В состав системы входят охранные извещатели, которые размещаются вдоль периметра участков местности, зданий и сооружений, в категорированных помещениях. При обнаружении нарушителя система формирует сигнал тревоги, фиксирующий место и время нарушения. Вся информация о сигналах тревоги и состоянии элементов системы архивируется на сервере системы контроля и управления доступа и может быть использована для анализа и прогнозирования складывающейся ситуации.

Система пожарной сигнализации предназначена для обнаружения возгорания, сопровождающегося повышенной температурой или выделением дыма, сбора, обработки, передачи и представления информации в систему управления и контроля доступа. В состав системы входят пожарные извещатели, которые размещаются в помещениях и функционируют круглосуточно.

Система видеонаблюдения предназначена для ведения дистанционного визуального контроля за ситуацией на участках охраняемой территории или в его режимных помещениях и для архивации видеoinформации в конкретные промежутки времени.

Система защиты информации представляет собой комплекс специальных средств и правил, обеспечивающих противодействие несанкционированному получению, искажению или уничтожению злоумышленниками конфиденциальной информации, хранимой на бумажных, магнитных носителях и в ПК, а также информации с закрытых совещаний и информации, передаваемой по различным каналам связи.

Система жизнеобеспечения объекта предназначена для контроля и поддержания нормального режима снабжения объекта электроэнергией,

освещением, чистым воздухом, а также контроля теплоснабжения, водоснабжения, радиационной обстановки и т. д. В помещениях объекта в необходимых случаях устанавливаются датчики ядовитых газов, температуры и уровня воды, дозиметры и терморегуляторы.

Персонал службы безопасности (руководитель службы, дежурный администратор базы данных, оператор сервера системы управления и контроля доступа, дежурные охранники, тревожная группа) защищает объект от внешних и внутренних злоумышленников, анализирует складывающуюся ситуацию, разрабатывает и реализует меры по снижению вероятности совершения злоумышленниками действий, ведущих к аварийным и чрезвычайным ситуациям или к значительному материальному ущербу.

Спецсредства досмотра, отражения и ликвидации угроз включают в себя: средства индивидуальной защиты персонала (бронежилеты, каски) и активной обороны (дубинки, газовое и огнестрельное оружие и т. д.), средства досмотра посетителей и транспорта, химические ловушки, автотранспорт и средства пожаротушения.

Процедурные средства представляют собой комплект организационно-распорядительной документации, который регламентирует деятельность персонала службы безопасности в процессе несения службы, при организации противодействия внешним и внутренним нарушителям, проведении аналитической работы по выявлению и предотвращению угроз объекту, взаимодействию с внешними организациями и службами. Этот комплект документов включает в себя: требования к персоналу, методику его тестирования и тренировки, тактические планы, оперативные процедуры, инструкции по управлению в кризисных и чрезвычайных ситуациях, в том числе при нарушениях общественного порядка. Эффективность деятельности персонала зависит от качества системы связи и используемых специальных и технических средств.

Система оперативной и громкоговорящей связи предоставляет возможности для централизованного управления сотрудниками, находящимися на различных участках объекта, обеспечивая службе безопасности необходимые мобильность и маневренность, а также служит для оповещения на объекте об аварийных и чрезвычайных ситуациях и управления действиями персонала в этих условиях.

Элементы строительных конструкций включают в себя: основное, вспомогательное и дополнительное ограждения, ворота и калитки периметра объекта, стены и перекрытия зданий.

Инженерные средства защиты объекта содержат: решетки оконных проемов, водозаборных и вентиляционных сооружений, подземных и наземных коммуникаций; металлические двери, ставни, замки и сейфы в помещениях; контрольно-пропускные пункты для прохода людей, автомобильного и железнодорожного транспорта.

В связи с широким использованием современных электронных компонентов и цифровых методов обработки информации в настоящее время происходит существенная «интеллектуализация» системы защиты объектов. Техническая система защиты объекта в общем случае состоит из следующих компонентов:

- сеть информационных датчиков-извещателей для получения полной информации о состоянии оперативной обстановки на объекте;
- исполнительные устройства, которые включаются автоматически или по команде оператора;
- пункты контроля и управления системой отображения информации, поступающей от сети датчиков, которые позволяют операторам управлять исполнительными устройствами и персоналом службы безопасности;
- центральный процессор (сервер) для накопления информации по всем вопросам безопасности и обеспечения заданных режимов работы элементов всей системы;
- коммуникации, обеспечивающие обмен информацией между всеми элементами системы и должностными лицами, участвующими в защите объекта.

2. Системы и средства охранно-пожарной сигнализации

В основе системы охраны объектов лежит принцип создания последовательных рубежей защиты, в которых угрозы должны быть своевременно обнаружены, а их распространению будут препятствовать надежные преграды. Такие рубежи защиты (зоны безопасности) должны располагаться последовательно – сначала основное ограждение территории объекта, затем территория объекта, отдельные здания объекта, коридоры и смежные помещения внутри зданий и, наконец, главное, особо важное помещение – хранилище материальных ценностей и информации.

Чем сложнее и надежнее защита каждой зоны безопасности, тем больше времени требуется на ее преодоление и тем вероятнее, что расположенные в зонах средства обнаружения угроз подадут сигнал тревоги, следовательно, у сотрудников охраны останется больше времени для определения причин тревоги и организации эффективного отражения и ликвидации угрозы.

Для обеспечения требуемой надежности обнаружения проникновения нарушителя на объект при разработке схемы охраны объекта используется концепция многорубежной сигнализации. Использование принципа многорубежной охраны позволяет практически исключить возможность обхода нарушителем одновременно всех рубежей сигнализации.

Важной составляющей частью системы охраны объекта являются технические средства охраны, которые образуют систему охранной сигнализации.

Охранная сигнализация – совокупность совместно действующих технических средств для обнаружения проникновения или попытки проникновения на

охраняемые объекты и (или) пожара на них; для сбора, обработки, передачи и представления в заданном виде потребителям информации о проникновении, неисправности или другой служебной информации.

В состав системы входят комплекс охранной сигнализации, устанавливаемый на охраняемом объекте, и система передачи извещений, приемная часть которой размещается в пункте охраны.

По принципу построения и виду охраняемого объекта охранная система может быть автономной или централизованного наблюдения. При использовании автономной сигнализации извещения с выхода одного объектового комплекса выдаются охранной системой на этом же охраняемом объекте в виде звуковых или световых сигналов тревоги. Субъектом автономной охраны является объективное подразделение охраны (сторож, пост милиции, частная охранная фирма, пожарное подразделение предприятия) или дежурная часть, например, органа внутренних дел, куда передается тревожное извещение.

Охранная система централизованного наблюдения применяется для контроля большого количества объектов, расположенных на расстоянии нескольких километров в пределах одного населенного пункта. Субъектом такой охранной системы являются подразделения вневедомственной охраны при органах внутренних дел.

Технические средства и системы контроля и управления доступом предназначены для контроля и санкционирования доступа людей, транспорта и других объектов в (из) помещения, здания, на территории. Такие современные системы с компьютерным управлением в соответствии с ГОСТом Р должны обеспечивать следующие функции:

- регистрацию и протоколирование тревожных и текущих сообщений;
- приоритетное отображение тревожных событий;
- управление работой преграждающих устройств в точках доступа по командам оператора;
- возможность задания временных режимов идентификаторов пользователей в точках доступа и уровней доступа;
- защиту от несанкционированного доступа к элементам управления, установки режимов и к информации;
- автоматический контроль исправности средств, входящих в систему, и линий передачи информации;
- возможность автономной работы контроллеров системы с сохранением ими основных функций при отказе связи с пунктом централизованного управления;
- установку с пункта управления режима свободного доступа при аварийных ситуациях и чрезвычайных происшествиях (пожар, землетрясение, взрыв и т. д.);
- осуществление в случае нападения блокировки прохода по команде с пункта управления;

- возможность подключения дополнительных средств специального контроля и досмотра.

Средства охранно-пожарной сигнализации классифицируются по двум признакам: области применения и функциональному назначению.

По области применения технические средства охранно-пожарной сигнализации делятся на три группы: 1) охранные; 2) охранно-пожарные; 3) пожарные.

По функциональному назначению они также подразделяются на три группы, включающие в себя средства:

1) обнаружения (извещатели), предназначенные для получения информации о состоянии контролируемых параметров (световой луч, СВЧ-поле, инфракрасное излучение и т. д.);

2) оповещения (приемно-контрольные приборы, оповещатели), предназначенные для приема и преобразования служебной и тревожной информации и выдачи оповещения;

3) передачи информации (системы передачи извещений в составе – оконечные устройства, ретрансляторы и пульта централизованного наблюдения), предназначенной для передачи по каналам связи, обработки и хранения информации (извещений о проникновении, служебных и контрольно-диагностических извещений, а также для передачи и приема команд телеуправления).

Извещатели охранные различают по виду контролируемой зоны (точечные, линейные, поверхностные и объемные) и принципу действия (магнитно-контактные, ударно-контактные, электроконтактные, звуковые, вибрационные, ультразвуковые, радиоволновые, комбинированные и т. д.).

В соответствии с нормативными требованиями, а также сложившейся практикой автоматические пожарные извещатели классифицируются по следующим основным признакам: вид контролируемого признака пожара, способ питания, принцип действия, вид зоны обнаружения.

Срабатывание автоматических извещателей происходит при достижении контролируемого параметра окружающей среды установленного порогового значения. В качестве контролируемых признаков пожара могут выступать: повышенная температура воздуха, выделение продуктов горения, турбулентные потоки горячих газов, электромагнитное излучение и др.

Основными характеристиками датчиков охранно-пожарной сигнализации (извещателей) являются чувствительность, инерционность, форма и размеры зоны обслуживания, помехозащищенность. Кроме того, немаловажны такие характеристики, как надежность, конструктивное исполнение для работы в установленных условиях окружающей среды, параметры электропитания, массогабаритные показатели и др.

3. Системы и средства защиты объектов уголовно-исполнительной системы

Основываясь на Законе Российской Федерации «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы», Уголовно-исполнительном кодексе Российской Федерации, Наставлении по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы и Руководстве по технической эксплуатации инженерно-технических средств охраны и надзора, применяемых для оборудования объектов уголовно-исполнительной системы, инженерно-технические средства охраны и надзора (ИТСОН) должны обеспечивать:

- необходимые условия для выполнения задач охраны минимальной численностью караулов в любое время суток и года;
- повышение эффективности работы персонала по поддержанию установленного порядка отбывания наказания;
- управление составом караула, дежурной смены при несении ими службы и действиях при чрезвычайных обстоятельствах;
- обнаружение осужденного (нарушителя) при различных способах преодоления им линии охраны или при его несанкционированном выходе (входе) из специальных зданий, таких как КПП, ПКТ и ШИЗО, административных зданий и помещений хранения товарно-материальных ценностей, транспортных средств;
- оповещение караула, дежурной смены, администрации объекта о нарушении линии охраны, несанкционированном выходе (входе) из специальных зданий и транспортных средств или об угрожающих действиях осужденных по отношению к лицам, находящимся на объекте;
- задержание осужденного в пределах запретной зоны объекта на время, необходимое для действий караула, дежурной смены и администрации объекта по предотвращению или пресечению побега;
- регистрацию (документирование) сигналов, распоряжений, команд и переговоров должностных лиц;
- установленный режим пропуска людей, условий для досмотра транспорта на КПП, обнаружение запрещенных предметов при попытке их проноса (передачи) через пункты контроля и утаивания, воспрепятствование перебросу через запретную зону;
- дистанционное наблюдение за территорией объекта охраны и поведением осужденных;
- условия для применения служебных собак на объекте охраны;
- изоляцию друг от друга групп осужденных в соответствии с установленным режимом их содержания;

- маскировку объекта и предупреждение осужденных и посторонних лиц о границах запретной зоны;
- управление лицами суточного наряда;
- подачу команд и распоряжений осужденным.

Учитывая эти требования, рассматриваемые средства можно условно разделить на инженерно-технические средства охраны и надзора и специальные технические средства охраны и обеспечения установленного режима.

Инженерно-технические средства охраны и надзора, в свою очередь, подразделяются на инженерные и технические средства.

Инженерно-техническими средствами оборудуются:

- объекты учреждений, исполняющих уголовные наказания, следственные изоляторы;
- транспорт для перевозки осужденных;
- специальные (военные) склады и базы.

Комплексное использование ИТСОН позволяет создать непреодолимый барьер для нарушителей. При этом технические средства гарантируют обнаружение нарушителя, а инженерные – максимально замедляют скорость его передвижения.

Инженерные средства охраны и надзора

К инженерным средствам охраны и надзора относятся:

- ограждения объектов охраны;
- сооружения и конструкции на постах;
- инженерные заграждения;
- сооружения и конструкции на контрольно-пропускных пунктах;
- сооружения и конструкции на внутренней территории объекта;
- средства механизации и автоматизации;
- сооружения и конструкции в транспортных средствах.

Ограждения объектов охраны

Ограждения применяются для выгораживания территории объектов уголовно-исполнительной системы, запретных зон и выводных коридоров. К ограждениям относятся заборы сплошного заполнения деревянной, кирпичной, железобетонной или смешанной конструкции, а также заборы из колючей проволоки или армированной скрученной колючей ленты (АСКЛ), металлической сетки, решетки и штакетника.

Таким образом, в зависимости от назначения ограждения объектов охраны подразделяются: на основное ограждение, ограждения запретных зон, выводных и просматриваемых коридоров, изолированных участков, снегозащитные заграждения.

Инженерное ограждение (забор) представляет собой комплексное сооружение, оборудованное противопобеговыми ограждениями типа «Шиповник» и «Егоза».

В практической деятельности учреждений, исполняющих наказания, противопобеговое ограждение «Шиповник» выполняется в нескольких вариантах. Один из них представляет собой забор, состоящий из опор, выполненных из стальных труб диаметром 10 см. Расстояние между опорами составляет 5 м. В середине опор под углом 45° привариваются трубы диаметром 5 см. Получается сооружение в виде буквы «Ж». К опорам и трубам крепится с помощью сварки металлическая сетка. Высота ограждения – 4 м.

Дальнейшей разработкой ограждения «Шиповник» является «Шиповник-М», изготавливаемый в двух вариантах.

Для городских объектов ограждение «Шиповник-М» представляет собой наклонное полотно из нитей армированной скрученной колючей ленты, расположенное на траверсах, и спирали (из АСКЛ), размещаемое по верху маскировочного забора. Для загородных объектов противопобеговое ограждение «Шиповник-М» выполняется на стойках, прикрепленных к железобетонным приставкам на линии ограждения внешней запретной зоны, и представляет собой вертикальное полотно из АСКЛ и спиралей в нижней и верхней его частях.

Система типа «Шиповник» обеспечивает задержание нарушителя, имеющего инструменты (кусачки, пассатижи и др.) или подручные средства (доски, трапы и т. п.) не более чем на 1 мин., а при их отсутствии – на 3–5 мин.

Ограждение «Егоза» представляет собой забор из АСКЛ.

Дальнейшей разработкой системы «Егоза» послужили системы «Багульник» и «Лимонник», предназначенные для блокировки козырька основных ограждений и включающие спираль из АСКЛ и размещенный в ней трибоэлектрический кабель-датчик.

Сооружения и конструкции на постах

К сооружениям и конструкциям на постах относятся:

- наблюдательные площадки, вышки, постовые грибы и будки;
- тропы нарядов и специалистов ИТСОН;
- контрольно-следовые полосы;
- разграничительные и контрольные знаки;
- оборонительные сооружения.

Наблюдательные площадки предназначены для несения службы часовыми при чрезвычайных обстоятельствах или для периодического осмотра ими запретной зоны и территории объекта. По конструктивному исполнению площадки могут быть неподвижными или шарнирно-откидными.

Наблюдательные вышки предназначены для размещения часовых при несении ими службы по охране объектов. Они могут быть стационарными и передвижными, деревянной, металлической или смешанной конструкции.

Тропы нарядов предназначены для передвижения: внешняя – лиц караула, внутренняя – контролеров. Тропа специалистов ИТСОН – это полоса местности, подготовленная для их передвижения при обслуживании инженерно-технических средств охраны и надзора.

Контрольно-следовой полосой (КСП) называется полоса местности, которая в естественном состоянии или после специальной обработки обеспечивает сохранение заметных отпечатков следов нарушителей.

Для обозначения границ постов и участков средств обнаружения применяются разграничительные знаки, а для обозначения их удаления от караульного помещения и времени прибытия к ним лиц караула – контрольные.

Оборонительные сооружения (окопы и укрытия) устраиваются вблизи наружных постов и караульных помещений по особому распоряжению.

Для служебных собак на объектах охраны оборудуются блокпосты и посты глухой привязки, которые предназначены для прикрытия труднопросматриваемых участков и направлений вероятного совершения побегов.

Инженерные заграждения

Инженерные заграждения – это сооружения и конструкции, устанавливаемые на местности в пределах запретных зон, в специальных зданиях, инженерных коммуникациях и внутри объектов охраны с целью затруднить осужденному совершение побега. Инженерные сооружения подразделяются на противопобеговые и противотаранные. По конструктивному исполнению они могут быть постоянными и переносными.

Сооружения и конструкции

на контрольно-пропускных пунктах

Контрольно-пропускным пунктом (КПП) называется место, оборудованное для проверки и пропуска людей и транспорта. На КПП, как правило, строится двухэтажное здание и оборудуется контрольная площадка.

Здание располагается вне территории объекта таким образом, чтобы его тыльная сторона совпадала с линией охраны (основным ограждением), в нем предусматриваются: караульное помещение, шлюз, проходной коридор; комнаты часового КПП, дежурного контролера, хранения и выдачи посылок, свиданий и обыска осужденных; операторская, щитовая, мастерская ИТСОН, аккумуляторная, щелочная и служебно-бытовые помещения учреждения.

КПП для пропуска железнодорожного транспорта устраивается в местах прохождения железнодорожных путей через запретную зону объекта и обычно состоит из здания (будки) и контрольной площадки.

Контрольные площадки предназначены для досмотра транспортных средств и располагаются внутри объекта у зданий КПП со стороны проходного коридора. Их размеры должны обеспечивать размещение досматриваемого автомобильного транспорта или не менее трех железнодорожных вагонов и иметь твердое покрытие. На площадке устанавливаются осветительные приборы, розетки для включения переносных светильников, средства служебной связи, вызывные устройства средств оповещения и оборудуется место для хранения инвентаря, используемого при досмотре.

Сооружения и конструкции на внутренней территории объекта

К сооружениям и конструкциям на внутренней территории объекта относятся:

- просматриваемые коридоры и изолированные участки;
- сооружения в здании ПКТ и ШИЗО;
- сооружения в здании оперативного дежурного;
- сооружения на постах секции внутреннего порядка;
- площадки для построения осужденных.

Средства механизации и автоматизации

Средства механизации и автоматизации предназначены для улучшения условий несения службы и повышения пропускной способности КПП. К ним относятся приводы различного назначения и конструкции, замковые и запорные устройства, путевые и конечные выключатели, кнопочные посты управления.

Средства механизации и автоматизации должны обеспечивать:

- дистанционное открывание и закрывание ворот, шлагбаумов;
- управление противотаранными устройствами, замковыми и запорными устройствами дверей;
- возможность перехода на ручное управление;
- надежность, безопасность и удобство обслуживания.

Кроме того, средства автоматизации должны обеспечивать автоматическую фиксацию и световую индикацию крайних положений ворот, шлагбаумов и противотаранных упоров.

Сооружения и конструкции в транспортных средствах

В деятельности органов, исполняющих наказания, наибольшее значение придается транспорту для перевозки осужденных, подозреваемых и обвиняемых в совершении преступлений. К таким транспортным средствам относятся:

- специальные и грузовые автомобили;
- специальные железнодорожные вагоны;
- грузовые железнодорожные вагоны;
- грузовые железнодорожные платформы;
- морские и речные суда.

Конструкция этих транспортных средств, а также оборудование их инженерно-техническими средствами предусматривает удобное размещение конвоя, предупреждение побегов во время перевозок и изоляцию перевозимых лиц друг от друга.

Технические средства охраны и надзора

К техническим средствам охраны и надзора относятся:

- средства обнаружения;
- средства тревожной сигнализации;
- системы и устройства сбора и обработки информации;
- средства видеонаблюдения;
- приборы контроля и досмотра;
- средства оперативной связи

Средства обнаружения

Средства обнаружения предназначены для подачи сигналов при попытке преодоления нарушителем линии охраны по периметру объекта с целью совершения побега и при несанкционированном выходе из специальных зданий ПКТ, ШИЗО, КПП или входе в специальные здания, сооружения, помещения, такие как магазин, аптека.

Средства обнаружения устанавливаются в запретной зоне объекта, на КПП и на внутренней территории объекта. Они подразделяются на стационарные и передвижные. Последние применяются для усиления охраны участков периметра, на которых наиболее вероятно совершение побегов, для оборудования временных объектов работ за пределами учреждения, при проведении розыскных мероприятий и т. д.

Средства обнаружения по физическим свойствам подразделяются на параметрические и генераторные.

Для параметрических средств характерно изменение каких-либо параметров электрических цепей, например, индуктивного или емкостного сопротивления при воздействии на эти средства нарушителем, в результате чего возникает выходной электрический сигнал, характеризующийся изменением силы тока, напряжения, амплитуды, частоты или фазы переменного тока. Эти средства обнаружения могут быть электромеханическими, емкостными, радиолокационными, ультразвуковыми, индуктивными, магнитоомическими, фотоэлектрическими и вибрационными.

В генераторных средствах обнаружения возникает электрический сигнал за счет преобразования какой-либо неэлектрической величины. Такие средства обнаружения делятся на вибрационные и тепलोкационные, обнаруживающие нарушителя путем приема и регистрации электромагнитного излучения тела человека.

Применение определенных средств обнаружения зависит от характера блокируемых объектов и их назначения. Можно выделить четыре основные группы средств блокирования:

- запретные зоны и другие охраняемые объекты, которые применяются для блокировки наземной и подземной части местности, прикрытия воздушного пространства над объектами, а также водных рубежей;
- стены, оконные проемы, решетки и жалюзи режимных корпусов;
- внутреннее пространство режимных корпусов и помещений;
- административные здания и помещения, в которых сосредоточены материальные ценности.

Для охраны периметра используется целый ряд технических систем, в основу работы которых положены различные принципы действия. Общим для всех систем является то, что каждая из них состоит из линейной части, устанавливаемой в запретной зоне объекта, и сложной стационарной аппаратуры, размещаемой в комнатах оператора ИТСОН и дежурной части. Для повышения эффективности охраны используется 3–4 рубежа охраны.

Так, при совершении побега через запретную зону осужденный встречает на своем пути линейную часть системы охраны. Ее первым рубежом обычно является телеемкостная система сигнализации, которая надежно срабатывает при приближении осужденного на определенное расстояние к ее линейной части. В основу работы системы положен эффект изменения емкости участка проволочного ограждения (забора) при приближении к нему человека. Телеемкостная система является очень эффективным техническим средством обнаружения, однако при ухудшении погодных условий (ветер, дождь, снег) система часто срабатывает от помех, и так как при этом выдается сигнал тревоги, состав караула постоянно должен на него реагировать.

Если осужденный преодолел телеемкостную систему, то на его пути встает следующая преграда – второй рубеж охраны. Таким рубежом обычно являются радиолучевые системы, представляющие собой радиолокатор, реагирующий на появление любого предмета на линии «передатчик–приемник».

Передатчик излучает радиолуч СВЧ-диапазона, который имеет зависящий от настройки определенный объем, то есть ширину, высоту, и направлен в сторону линии охраны к приемной части. В результате образуется чувствительная зона, невидимая осужденному, совершающему побег. При пересечении луча человеком происходит уменьшение энергии луча, проходящего в приемную часть, и выдается сигнал тревоги. Ослабление энергии луча происходит за счет интерференции (наложения) прямого луча и отраженного от человека сигнала.

Отметим, что радиолучевые датчики имеют вблизи приемной части небольшие участки, которые не перекрыты невидимыми лучами. Это так называемые мертвые зоны. Осужденный может пройти около приемной или передающей части пригнувшись и, следовательно, не пересечь луч. Для недопущения этого по всему периметру охраны антенные пары системы

устанавливаются с некоторым сдвигом по отношению к другим парам, и таким образом «мертвые зоны» одной пары перекрываются лучами другой и т. д.

В настоящее время созданы принципиально новые радиолучевые системы на основе радиоизлучающего кабеля РИ-50-7-11. Их преимущество по сравнению с ранее рассмотренными системами состоит в отсутствии «мертвых зон». Датчик на основе такого кабеля обладает высокой надежностью. Им можно блокировать участки местности, проходящие по сложному рельефу. Он не реагирует на объекты малой массы (до 15 кг). Принцип работы датчика заключается в регистрации изменения электромагнитного поля, которое создается между излучающим и приемным кабелями при вторжении нарушителя в контролируемую зону. Один комплект такого радиоволнового устройства обеспечивает охрану периметра протяженностью 600 м (шесть участков по 100 м каждый). Размер контролируемой зоны по ширине до 3 м, а по высоте над поверхностью грунта – до 1 м.

Преодолев две системы обнаружения, осужденный может оказаться у основного ограждения объекта.

Третьим рубежом охраны является контактно-вибрационная система, которая используется для блокировки основного ограждения и его козырька.

Линейная часть этой системы представляет собой изолированные провода, расположенные на расстоянии 20 см друг от друга по всей высоте периметра охраны. При попытке преодоления основного ограждения осужденный вынужден раздвигать провода или обрывать их. В любом случае система срабатывает, и поступает сигнал об обнаружении.

Преодолеть систему незаметно практически невозможно. Однако при плохих метеорологических условиях система срабатывает от помех, но в количественном отношении таких срабатываний у нее гораздо меньше, чем у телеемкостных систем, приблизительно в 6–8 раз.

Рассмотрев три системы обнаружения, которые при одновременном применении практически исключают незаметное совершение побега осужденным, заметим, что остается еще возможность его совершения путем подкопа под запретной зоной. Для исключения этого применяются противоподкопные системы.

Современные противоподкопные системы, линейная часть которых устанавливается под землей на глубину до 0,8 м и от основного ограждения на 0,5 м, имеет в своей основе сейсмические датчики. Такие датчики улавливают колебания почвы и преобразуют их в электрические сигналы. Если осужденный пытается совершить побег путем подкопа под основным ограждением, на стационарной аппаратуре выдается сигнал тревоги с указанием места нарушения с точностью до 25 м. Кроме того, с помощью этой системы можно прослушать характер колебаний и даже услышать разговор осужденных, осуществляющих подкоп. Такие системы производят селекцию механических колебаний, связанных с работой шанцевым инструментом, от посторонних

колебаний, вибрации почвы, например, при движении транспорта, работе обрабатывающих станков.

Система позволяет заблокировать до 800 м периметра (4 участка по 200 м) и обнаружить нарушителя, ведущего подкоп под запретной зоной на глубине до 3 м.

Таким образом, преодолеть незаметно линейные части 3–4 рубежей охраны практически невозможно. Поэтому осужденные, совершающие побег через запретные зоны, рассчитывают на то, что преодолеют эти рубежи быстрее, чем часовые выйдут на их перехват.

Средства тревожной сигнализации

Эти средства предназначены для подачи светового и звукового сигналов о нападении, чрезвычайных обстоятельствах на объектах охраны, для вызова должностных лиц, а также сбора личного состава по тревоге.

Средства оповещения состоят из вызывных устройств (извещателей, кнопок, тумблеров), приемных аппаратов (звонков, ревунов, сирен, громкоговорителей) и соединительных линий.

Приемные аппараты могут входить в состав пульта управления техническими средствами охраны и надзора или устанавливаться отдельно. Для визуального отображения информации и контроля за поступающими сигналами применяются мнемосхемы (световые табло, дисплеи компьютеров).

Системы и устройства сбора и обработки информации

На каждом объекте охраны, как правило, одновременно используется значительное количество средств обнаружения, обеспечивающих охрану периметра, режимных корпусов, служебных кабинетов и иных помещений. Информация о различного рода нарушениях должна поступать в дежурную часть и там отображаться в наглядном виде. Для этого датчики подключаются к приемно-контрольным устройствам – концентраторам.

Концентраторы обеспечивают:

- одновременный прием сигнала тревоги со всех участков (помещений) охраняемого объекта, где установлены датчики средств обнаружения, индикацию сигналов путем включения номерных ламп, звуковую сигнализацию, включение общестанционной (выносной) лампы и счетчика сигналов тревоги;

- возможность увеличения емкости за счет добавления к базовому блоку линейных блоков;

- автоматический переход на питание от резервного источника в случае отключения основного.

Современные компьютеризированные системы используются для сбора, обработки и документирования информации с периферийных устройств, датчиков, извещателей, устройств ограничения доступа, приборов контроля и надзора. Кроме того, данные системы обеспечивают оперативную связь дежурного (оператора ИТСОН) с руководством, службами и подразделениями учреждения, а также с постовыми контролерами, автоматическую запись всех сигналов и команд, телефонных переговоров, громкоговорящее оповещение на периметре и в помещении резервной группы, автоматическое включение освещения нарушенного участка периметра.

Системы контроля доступа применяются для выполнения требований режима в учреждении, повышения пропускной способности КПП, обеспечения безопасности дежурного персонала. Системами контроля доступа и дистанционного открывания дверей оборудуются режимные помещения учреждения, изолированные участки, ПКТ и ШИЗО, ЕПКТ, ДИЗО, одиночные камеры в исправительных колониях особого режима, КПП. Станционные устройства располагаются на местах несения службы инспекторами дежурной смены, в помещениях оператора пульта управления техническими средствами охраны, оператора пульта управления техническими средствами надзора, часового КПП, оперативного дежурного учреждения.

Средства видеонаблюдения

Средства видеонаблюдения применяются для дистанционного наблюдения за обстановкой в охраняемых зонах, на территории объекта, в режимных зданиях и помещениях, на подступах к территории учреждения.

С помощью современных систем видеонаблюдения обеспечивается:

- наблюдение различных контролируемых зон с оценкой их текущего состояния;
- обнаружение вторжения в охраняемые зоны;
- запись изображения контролируемых зон с возможностью последующего анализа происшедшего и идентификации личности нарушителя;
- осуществление визуальной проверки охраняемой зоны при срабатывании систем охранно-пожарной сигнализации.

Приборы контроля и досмотра

Приборы контроля и досмотра применяются для обеспечения надлежащего контроля и досмотра людей и транспорта на предмет обнаружения сокрытых запрещенных предметов.

Приборы досмотра рентгеновские применяются для досмотра крупноформатных объектов (предметов) малой плотности с целью выявления недопустимых вложений.

Средствами и приборами контроля и досмотра оборудуются помещения для обыска и приема лиц под стражу, санпропускники между жилой и производственной (хозяйственной) зонами, КПП.

Средства оперативной связи

К средствам оперативной связи относятся соединительные линии связи, абонентские устройства, установки громкоговорящей связи, устройства телефонной и других видов связи в системах технических средств охраны.

Вид и способ оперативной связи определяются начальником учреждения и зависят от характера выполняемых подразделением задач.

Оперативная связь в учреждении УИС обеспечивается силами и средствами учреждения УИС.

Системы связи и контроля на автотранспорте применяются для блокировки и контроля состояния дверей и люков специальных автомобилей и осуществления двухсторонней телефонной связи между лицами караула, находящимися в кабине и кузове.

В целях создания предусмотренных законом условий для проведения краткосрочных свиданий, а также воспрепятствования непосредственных контактов заключенных под стражу и осужденных к лишению свободы с посетителями комнаты свиданий оборудуются специальными кабинетами с переговорными устройствами.

Устройства обеспечивают индивидуальный контроль над проведением переговоров во время свиданий и их аудиозапись. Такие устройства состоят из пульта управления с блоком питания и усилителя. На пульте имеются тумблеры для подключения переговорных кабин и звукозаписывающей аппаратуры, а также головных телефонов для прослушивания конкретных переговоров.

К усилителю переговорного устройства подключаются три динамика, один из них устанавливается в комнате посетителей, а два других – в комнате свиданий (со стороны кабин посетителей и осужденных). Динамики используются для объявлений о порядке свиданий.

Кабины для посетителей оборудуются двумя-тремя телефонными трубками, а для осужденных – одной.

К средствам оперативной связи также можно отнести устройства прямой односторонней громкоговорящей связи дежурного по корпусному отделению с камерами. Данные устройства обеспечивают возможность передачи необходимой информации в камеры с использованием линий местной радиотрансляционной сети с рабочего места дежурного по корпусному отделению. Устройство состоит из пульта управления и громкоговорителей, устанавливаемых в камерах, линий радиосети и соединительных кабелей. На панели пульта имеются тумблеры управления и микрофон. С пульта производится также включение местной радиосети для трансляции в камеры.

Лекция 4. ОСНОВЫ ОРГАНИЗАЦИИ СВЯЗИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

- 1. Система связи правоохранительных органов.*
- 2. Сеть связи.*
- 3. Управление системой связи в УИС.*

1. Система связи правоохранительных органов

Успех в борьбе с преступностью во многом зависит от уровня технической оснащённости правоохранительных органов, на которые возложено проведение оперативно-розыскных мероприятий и следственных действий, содержание заключённых под стражей и т. д.

Исход расследования любого происшествия находится в тесной связи с вопросом о своевременности и эффективности выполнения самых первых действий оперативного характера, обеспечивающих раскрытие преступления. Именно первоначальная стадия работы по делу позволяет реализовать наибольшие возможности для сбора необходимых данных о преступнике, его обнаружения, преследования и задержания. Не случайно ещё в древнем уголовном праве придавалось важное значение такому мероприятию, как «гнать по следу». Раскрытие преступлений по горячим следам не утратило своего значения до сих пор.

Таким образом, важнейшим фактором оперативной работы, как, впрочем, и следственной, является быстрота, что в значительной мере определяется чёткостью взаимодействия оперативных работников, выполняющих какое-либо задание, связанное с установлением, розыском и задержанием скрывшегося преступника. Совершенно очевидно, что обеспечить надлежащую чёткость взаимодействия невозможно без хорошо налаженной связи.

Нередко преступник разыскивается одновременно несколькими группами оперативных работников, действующими в разных направлениях. Иногда одной из групп в момент поиска удается получить важную дополнительную информацию, например, о возможности нахождения преступника в определенном месте района действия другой группы. Наличие средств связи, особенно радиосвязи, позволяет быстро передать этой группе нужные сведения. Подобная информация после направления оперативных групп для выполнения задания может поступить к руководителю поиска, координирующему деятельность всех групп.

Следует отметить важную роль средств радиосвязи применительно к организации прочесывания местности в затруднительных условиях: на обширной территории со сложным рельефом, лесными массивами, в крупных

населенных пунктах и т. д. Наличие радиосвязи между поисковыми группами дает возможность своевременно оценивать обстановку и полноту обследования местности, уточнять и изменять маршруты и, таким образом, повысить эффективность оперативного мероприятия. Радиосвязь способствует также четкой координации действий моторизованных групп и пеших патрулей.

Трудно переоценить значение связи между следственными и оперативными группами, участвующими в обысках, которые проводятся в разных местах в одно время. Внезапные одновременные обыски у всех соучастников преступления или у обвиняемого и его родственников нередко дают положительные результаты. Такой метод лишает обвиняемого возможности принять меры по сокрытию искомых предметов после неудачно проведенного только в одном месте обыска. Средства связи, имеющиеся у этих групп, позволяют им своевременно обмениваться информацией о ходе и результатах обысков, что может значительно повысить результативность дальнейших действий.

Еще более результативным средством оперативной связи является телевидение. Его информационная емкость значительно больше, чем радио. Так, в следственной и оперативной работе иногда возникает необходимость срочно послать в определенное место сообщение, касающееся конкретного лица или предмета. Понятно, что никакое словесное описание не может сравниться с изображением объекта, обладающим фотографической точностью, а также позволяющим передавать динамику его движений. Например, средства телевидения в сочетании с прибором ночного видения дают возможность наблюдать за объектами в темное время суток и передавать изображение на пункт наблюдения, при этом оперативный работник следит за объектами, находясь в помещении перед экраном телемонитора.

Широко практикуется использование общественных телевизионных каналов. Зрителям обычно демонстрируют внешность разыскиваемого преступника или жертвы убийства и просят сообщить в органы внутренних дел, если кому-нибудь что-либо известно о них. Таким путем неоднократно удавалось установить личность преступников и потерпевших.

Итак, связь в системе правоохранительных органов является основным средством, обеспечивающим постоянное управление ими и их подразделениями.

Оптимальность управления во многом зависит от своевременности получения осведомительной информации от населения, учреждений, организаций, соответствующих подразделений правоохранительных органов, а также отдельных сотрудников этих органов. Она позволяет анализировать оперативную обстановку, быстро принимать необходимые меры, оперативно управлять подразделениями и службами, организовывать взаимодействие между органами правопорядка и их отдельными службами и координировать их действия. Решение этих вопросов во многом зависит от четкой организации

прямой и обратной связи, в том числе от того, насколько быстро доводятся до исполнителей управленческие решения.

Применение средств связи способствует эффективному управлению на стадиях получения осведомительной информации и передачи управленческих решений.

Средства связи позволяют в любое время года и суток, в любую погоду получить и передать информацию, управлять подразделениями и службами органов правопорядка.

Связь – это неотъемлемая часть системы управления правоохранительными органами. Она обеспечивает надежную, своевременную и качественную передачу всех видов информации в интересах управления ее субъектами. Организация связи обуславливается структурой субъектов правоохранительных органов, спецификой их деятельности, необходимостью взаимодействия и внутри системы, и вне ее – с другими министерствами и ведомствами.

Система связи правоохранительных органов является технической основой системы управления этих органов, ее информационной инфраструктурой. Она предоставляет руководству правоохранительных органов возможность своевременно и гарантированно доводить управленческие решения до подчиненных, осуществлять сбор информации в любых условиях оперативной обстановки.

Для обеспечения управления конкретным субъектом правоохранительных органов создается его объединенная система связи как совокупность территориальной системы, мобильных узлов и специальных систем связи.

Территориальная система связи базируется на сети связи общего пользования, стационарных опорных сетях связи главных управлений (министерств) и территориальных органов конкретных субъектов правоохранительных органов. Создаваемая по территориально-зонавому принципу система характеризуется высокой степенью независимости по отношению к структурным изменениям, происходящим в системе управления. Территориальная система связи наращивается за счет приема каналов из сети связи общего пользования, а также использования подвижных (мобильных) узлов связи.

Мобильные узлы связи обеспечивают управление силами субъектов правоохранительных органов, действующими в отрыве от мест постоянной дислокации, при проведении оперативно-розыскных мероприятий и возникновении чрезвычайных ситуаций.

Специальные системы связи предназначены для поддержания шифрованной и конфиденциальной связи руководства и решения специфических задач в интересах оперативных служб.

Структура системы связи включает в себя подсистемы:

- управления – органы управления связью;
- доставки сообщений – сети электро- и почтовой связи;
- обеспечения связи.

Задачи управления предъявляют к системе связи следующие требования: своевременность, надежность, достоверность, достаточная пропускная способность и скрытность передачи информации.

Своевременность связи – это способность обеспечивать передачу (прием) сообщений в сроки, определяемые оперативной обстановкой.

Надежность связи – способность обеспечить непрерывное управление в любых условиях оперативной обстановки.

Достоверность – способность связи обеспечивать воспроизведение передаваемых сообщений в пунктах приема с заданной точностью.

Пропускная способность системы связи – возможность передачи определенных объемов информации в единицу времени.

Скрытность связи – это сохранение в тайне содержания передаваемой информации и сам факт ее передачи.

Электросвязь (электрическая связь) представляет собой всякую передачу или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам.

Сеть почтовой связи представляет собой совокупность объектов почтовой связи и почтовых маршрутов операторов почтовой связи, обеспечивающих прием, обработку, перевозку (передачу), доставку (вручение) почтовых отправлений, а также осуществление почтовых переводов денежных средств.

2. Сеть связи

Взаимоувязанная сеть связи Российской Федерации представляет собой комплекс технологически сопряженных сетей связи общего пользования и ведомственных сетей электросвязи, расположенных на территории России, обеспеченный общим централизованным управлением, независимо от ведомственной принадлежности и форм собственности.

Под *сетью электросвязи* следует понимать технологические системы, обеспечивающие один или несколько видов передачи: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ПК, телевизионное, звуковое и иные виды радио- и проводного вещания.

Сеть связи общего пользования – это составная часть взаимоувязанной сети связи Российской Федерации, открытая для пользования всем физическим лицам, в услугах которой этим лицам не может быть отказано.

Ведомственные сети связи – сети электросвязи министерств и иных федеральных органов исполнительной власти, создаваемые для удовлетворения производственных и специальных нужд, имеющие выход на сеть связи общего пользования.

Материальной основой для создания сети связи являются средства связи – технические устройства, применяемые для формирования, обработки, передачи

или приема сообщений электросвязи либо почтовых отправлений, то есть средства связи вместе со средствами компьютерной техники составляют техническую базу обеспечения процесса сбора, обработки, накопления и распространения информации.

Сети связи правоохранительных органов строятся по радиально-зональному принципу. В структуру связи ее конкретного субъекта входят:

- пункт управления сетью (администратор сети);
- узлы связи: центральный; территориальный; подразделений (учреждений); запасных пунктов;
- линии связи: линии прямой связи; линии привязки; арендованные каналы и тракты;
- техническое обеспечение: межрегиональные восстановительные базы (ремонтные центры и т. п.); отделения ремонта узлов связи; склады.

Таким образом, в составе ведомственной сети функционируют центральный и территориальные узлы связи в субъектах Российской Федерации, а также линии (каналы) связи, организованные между ними.

Узел связи представляет собой организационно-техническое объединение сил и средств связи для образования и коммутации каналов, обмена сообщениями с абонентами сетей связи и сопряжения сетей связи между собой.

Центральные узлы субъектов правоохранительных органов структурно входят в состав своих центральных органов и предназначены для обеспечения всеми видами связи руководства и структурных подразделений. Центральный узел связи является главным узлом ведомственной сети связи, на него возлагается функция администрирования сети. В вопросах обеспечения связи ему подчинены все узлы связи территориальных органов.

Узлы связи территориальных органов (министерств, управлений) предоставляют услуги их руководству, структурным подразделениям и обеспечивают связь:

- с подчиненными подразделениями (учреждениями, органами);
- отдельно дислоцированными подразделениями (специального назначения, охраны, конвоирования, формируемыми по необходимости сводными отрядами, подвижными узлами связи и др.);
- взаимодействующими службами (воинскими частями, структурами местного самоуправления и т. д.).

Центральный и территориальный узлы связи организационно состоят из центров (отделов), отделений и групп. На центры возлагаются задачи по обеспечению определенного вида связи (внутренней связи, каналообразования, специальной связи и т. д.). Отделения (группы) выполняют вспомогательные функции и организационно входят в состав центров либо являются отдельными подразделениями узлов связи (отделение мобильной связи, группа радиосвязи и т. д.).

Для удовлетворения потребностей сети связи в средствах связи, поддержания их в постоянной готовности к применению, обеспечения безотказной работы, быстрого восстановления и возврата в эксплуатацию используются межрегиональные ремонтно-восстановительные базы (мастерские), отделения ремонта узлов связи и склады территориальных органов управления или центров инженерно-технического обеспечения (ЦИТО).

Для выполнения задач по обеспечению связью узлы связи соединены *линиями связи*, под которыми понимают физическую среду распространения электромагнитных волн (металлический или оптический кабель, атмосфера), обеспечивающую передачу сигналов электросвязи (радио-, радиорелейных, проводных, спутниковых и др.)

Линии прямой связи развертываются непосредственно между узлами связи конкретного субъекта правоохранительных органов.

Линии привязки соединяют узлы связи субъектов правоохранительных органов с узлами операторов связи или узлами взаимодействующих министерств (ведомств) для приема в эксплуатацию арендуемых каналов.

Канал – это совокупность среды распространения, оконечной и коммутационной аппаратуры связи, обеспечивающая передачу сообщения от его источника получателю. В зависимости от вида сообщения каналу присваивают название (телефонный канал связи, телеграфный канал связи, канал передачи данных). По территориальному признаку канал электросвязи может быть междугородным, магистральным, зонавым, местным. Каналу связи присваивают название «аналоговый» или «цифровой» в зависимости от метода передачи сигналов электросвязи, а если на разных его участках используются аналоговые или цифровые методы передачи сигналов электросвязи, то – «смешанный аналого-цифровой канал передачи». Цифровому каналу, в зависимости от скорости передачи сигналов электросвязи, присваивают названия: «основной», «первичный», «вторичный», «третичный», «четвертичный».

Среда распространения сигналов электросвязи или применяемых средств позволяет различать проводную, радио-, радиорелейную, тропосферную, спутниковую, оптико-электронную связь и др. В системе связи правоохранительных органов наибольшее распространение и применение нашли проводная, радио-, радиорелейная и спутниковая связь.

Проводная связь – электросвязь, в качестве среды распространения которой используются проводные (металлические или волоконно-оптические) линии связи. Система связи строится в основном на проводных каналах связи, арендуемых у операторов взаимоувязанной сети связи России. Заметим, что проводные линии занимают значительное место в структуре ведомственных сетей связи.

Радиосвязь – электросвязь, осуществляемая посредством радиоволн. Для организации радиосвязи используются ультракоротковолновые (УКВ) и

коротковолновые (КВ) радиостанции. Тип, мощность радиостанций и рабочие частоты определяются схемой организации радиосвязи.

Основной способ организации связи – это радиосеть с возможностью связи «каждого с каждым». При необходимости радиосвязь организуется по радионаправлениям, для увеличения ее дальности используются ретрансляторы.

При наличии в регионе технической возможности и средств для оперативной связи руководства правоохранительных органов используется сотовая, транкинговая (радиотелефонная связь с автоматическим предоставлением ограниченного числа каналов радиосвязи большому числу пользователей) и пейджинговая радиосвязь.

Радиорелейная связь – радиосвязь, осуществляемая с использованием радиорелейных систем передачи и основанная на ретрансляции радиосигналов на дециметровых и более коротких радиоволнах. Например, радиорелейная линия связи может быть образована из двух радиорелейных станций (однопролетная радиорелейная линия). Радиорелейная связь может обеспечивать привязку узлов связи территориальных органов управления и подразделений к узлам связи взаимоувязанной сети связи, а также применяться для организации линий прямой связи с отдельно дислоцированными подразделениями и учреждениями.

Спутниковая связь – радиосвязь между наземными радиостанциями, осуществляемая посредством ретрансляции радиосигналов через один или несколько спутников Земли. Спутниковая (космическая) связь с использованием портативных телефонов может применяться для связи с территориальными органами в регионах со сложной оперативной обстановкой, запасными пунктами управления в особый период, при авариях, нарушивших работу сети связи общего пользования. Использование спутниковой связи, например, целесообразно для обмена информацией между подразделениями уголовно-исполнительной системы и органов внутренних дел при конвоировании на железнодорожных и отдельных автомобильных маршрутах, а также определения их координат и направления движения.

По виду передаваемого сообщения связь подразделяют на телефонную, телеграфную, факсимильную, передачи данных, телевизионную, почтовую.

Телефонная связь – передача речевых сообщений по каналам электросвязи.

Телеграфная связь – передача документированных сообщений в виде буквенно-цифрового текста.

Факсимильная связь – передача по линиям связи печатных, рукописных, графических и других неподвижных изображений плоских оригиналов с воспроизведением их копий в пунктах приема.

Передача данных – это обмен информацией между вычислительными комплексами, локальными сетями и отдельными ПК по каналам электросвязи.

Телевизионная связь – передача по линиям электросвязи неподвижных и подвижных изображений действий наблюдаемых объектов.

Почтовая связь – доставка почтовых сообщений и периодической печати.

Наибольшее распространение вследствие оперативности, достоверности и доступности в правоохранительных органах получила телефонная связь. Для ведения переговоров используются правительственная междугородная связь (ПМ), ведомственные сети телефонной шифрованной связи, междугородная связь по арендованным и собственным каналам связи, местная и междугородная (автоматическая и заказная) связь по телефонной сети общего пользования, внутренняя телефонная сеть территориальных органов, а также телефонные сети взаимодействующих министерств и ведомств.

Традиционная телеграфная связь сохраняет свою значительную роль в информационном обмене. Она осуществляется с узлов (пунктов) связи, подключенных к сети абонент-ского телеграфирования. В настоящее время на телеграфных сетях связи внедряются современные технические средства на базе вычислительной техники, что позволяет автоматизировать процесс обработки потоков документальной информации.

Оперативный обмен служебными документами возможен по телефонной сети с использованием факсимильных аппаратов. Сообщение при использовании данного вида связи может непосредственно поступать на рабочее место должностного лица.

В настоящее время растет спрос на услуги документальной электросвязи, предоставляемые с использованием сетей передачи данных. Современные технологии обеспечивают широкий набор услуг: электронная почта, доступ к информационным ресурсам баз данных, передача документальных, видео- и голосовых сообщений, телеконференции, аудио- и видеоконференцсвязь.

Внедрение шифрованной связи обеспечивает передачу сведений, содержащих государственную и служебную тайну, между субъектами правоохранительной деятельности, взаимодействующими министерствами и ведомствами.

Правоохранительные органы являются пользователями и почтовой связи, находящейся под юрисдикцией Российской Федерации. Этот вид связи представляет собой единую технологическую сеть учреждений и транспортных средств, обеспечивающих прием, обработку, перевозку и доставку почтовых отправлений, перевод денежных средств, а также организующих на договорной основе экспедирование, доставку и распространение периодической печати.

3. Управление системой связи в УИС

Управление системой связи заключается в своевременном проведении мероприятий по организации связи, ее материально-техническом обеспечении, подготовке сил и средств связи к выполнению их предназначения, в том числе к действиям при осложнении оперативной обстановки, проведении розыскных мероприятий и чрезвычайных ситуациях.

Так, например, функционально-структурное обеспечение управления связью в уголовно-исполнительной системе подразумевает, что общее управление связью в УИС осуществляет директор Федеральной службы исполнения наказаний, в территориальных органах УИС – начальники управлений, учреждениях УИС – начальники учреждений.

Непосредственное руководство системой связи в Федеральной службе исполнения наказаний осуществляет отдел связи, в территориальных органах УИС – подразделения управленческих аппаратов инженерно-технического обеспечения (ИТО), связи и вооружения (отделы, отделения), в учреждениях УИС – старшие инженеры (инженеры) связи либо должностные лица, назначенные приказом начальника учреждения.

На управление системой связи возлагаются следующие задачи:

- планирование развития и совершенствования системы связи;
- организация связи и поддержание ее в рабочем состоянии;
- организация материально-технического обеспечения системы связи;
- проведение специальной подготовки сотрудников;
- подготовка системы связи к действиям при обострении оперативной обстановки, проведении розыскных мероприятий, чрезвычайных ситуациях;
- контроль функционирования системы связи.

Планирование системы связи – это деятельность должностных лиц, направленная на решение комплекса задач по определению способов построения и обеспечения функционирования системы связи, разработку планирующих, рабочих и распорядительных документов. Планирование может быть перспективным и текущим. Оно осуществляется исходя из задач, выполняемых субъектом правоохранительной деятельности, и имеющихся возможностей.

Перспективное планирование включает в себя разработку:

- в федеральном органе – концепций технической политики и перспективного плана развития (совершенствования) системы связи со сроком реализации до 5 лет;
- в территориальных органах – перспективных планов развития (совершенствования) системы связи с аналогичным сроком реализации.

Все перспективные планы согласовываются с вышестоящими органами управления и утверждаются начальниками, осуществляющими руководство связью.

Ежегодно в территориальных органах управления разрабатывается *план связи*. Он содержит: схему организации связи; схему организации радиосвязи; схему организации проводной и радиорелейной связи; расчет сил и средств связи.

Схема организации связи должна отображать структуру территориальной системы связи, узлы связи и направления связи, центры (пункты) коммутации, каналы взаимодействия. На схеме отмечаются каналы связи без учета способов их формирования и операторов, предоставивших каналы в аренду.

На схеме связи целесообразно указывать типы средств связи, режимы работы радиосредств, распределение каналов, количество корреспондентов в сети, радиостанции с дистанционным управлением и ретрансляторы (для радиостанций с дистанционным управлением – виды соединительных линий).

На схеме проводной и радиорелейной связи отображаются типы каналообразующей аппаратуры, распределение каналов, способы их коммутации и транзита, расчеты трасс связи, аппаратура привязки и места ее установки.

Схемы организации радио-, проводной и радиорелейной связи разрабатываются на карте или отдельных листах бумаги. При небольшом количестве каналов и линий связи схемы могут совмещаться в одном документе.

К схемам организации радио- и радиорелейной связи разрабатываются радиоданные, которые содержат:

- номера радиосетей;
- циркулярные и индивидуальные позывные радиостанций и корреспондентов;
- рабочие и запасные частоты (номера каналов, волн);
- типы радиосредств и места их нахождения;
- серии и номера таблиц, из которых набраны позывные корреспондентов;
- срок действия радиоданных;
- номера и даты выдачи разрешений на использование частот и позывных.

Выделение частот производят штабы военных округов Министерства обороны, МВД (ГУВД, МВД) республик (краев, областей) по заявкам.

Следует отметить, что применение произвольно назначенных частот и позывных запрещается, виновные в их использовании привлекаются к ответственности согласно действующему законодательству.

Во всех документах плана предусматривается обеспечение связи при обострении оперативной обстановки, проведении розыскных мероприятий и чрезвычайных ситуациях.

Кроме плана связи на год, в подразделениях на узлах связи разрабатываются месячные, квартальные и полугодовые планы работы. На незапланированные мероприятия готовятся отдельные схемы организации связи.

Для организации связи и поддержания ее в рабочем состоянии в каждом территориальном органе управления готовится *распоряжение по связи*. Оно разрабатывается на предстоящий год на основе распоряжения и плана связи вышестоящего органа управления (министерство, главное управление и т.д.) и доводится до исполнителя не позднее декабря текущего года.

При разработке распоряжения по связи учитываются:

- потребность в связи подразделений при выполнении ими служебных и производственных задач;
- функции специальных подразделений;

- возможный характер оперативно-розыскных мероприятий, действий при осложнении оперативной обстановки и чрезвычайных ситуациях;
- укомплектованность и техническое состояние средств связи;
- готовность узлов связи к обеспечению связи;
- необходимость связи взаимодействия с другими правоохранительными органами, органами местного самоуправления, сводными отрядами специального назначения и иными привлекаемыми силами и средствами.

В распоряжении по связи территориального органа указываются:

- пункты управления, режимы их работы и порядок связи с ними;
- организация связи с подчиненными подразделениями (проводная, радиорелейная, радио-, спутниковая);
- организация связи при проведении оперативно-розыскных мероприятий, обострении оперативной обстановки, чрезвычайных ситуациях;
- порядок осуществления связи взаимодействия;
- режимы работы средств связи;
- мероприятия по обеспечению безопасности связи.

Материально-техническое обеспечение системы связи заключается в проведении комплекса мероприятий, направленных на укомплектование подразделений связи техникой, организацию ее эксплуатации и ремонта. Вопросы материально-технического обеспечения регламентируются ведомственными нормативно-правовыми актами.

В целях подготовки системы связи к действиям при обострении оперативной обстановки, проведении мероприятий и чрезвычайных ситуациях органы управления связью участвуют в разработке необходимых планов действий подразделений.

Контроль за функционированием системы связи осуществляется в целях поддержания всех компонентов ведомственной сети связи в готовности к выполнению возложенных на них задач в установленные сроки, с необходимым качеством. Порядок контроля и критерии оценки определяются ведомственными нормативными актами.

В процессе управления должны учитываться особенности организации связи в различных низовых (подчиненных) подразделениях.

Связь в учреждениях уголовно-исполнительной системы (исправительных и воспитательных колониях, тюрьмах, следственных изоляторах, лечебных исправительных учреждениях) организуется на основании распоряжения по связи территориальных органов уголовно-исполнительной системы силами и средствами этих учреждений. При этом аппаратура и оборудование связи устанавливаются в специальных помещениях или комнатах оперативных дежурных, караулах, подразделениях охраны, исключая доступ к ним осужденных и посторонних лиц.

Для оперативного руководства в подразделениях на обслуживаемых территориях развертываются собственные сети телефонной связи. Для

организации такой связи используются автоматические телефонные станции, пульты оперативной связи, коммутаторы.

Также в учреждениях УИС и дежурных частях горрайорганов внутренних дел, например, могут развертываться сети громкоговорящей связи и радиотрансляции оповещения, устанавливаться переговорные устройства и другая аппаратура связи, обеспечивающая наиболее благоприятный режим функционирования.

Для управления подвижными нарядами используется ультракоротковолновая радиосвязь.

При осложнении оперативной обстановки на территории, обслуживаемой подразделением, связь с ним обеспечивается на приоритетной основе. Немедленно проверяются и вводятся в действие резервные каналы связи на этом направлении. Уточняется расчет личного состава узла связи органа управления и усиливается дежурная смена. Обеспечивается организация прямого канала связи узла связи и центрального узла связи, например, МВД и горрайоргана (при наличии возможности). Резерв средств связи приводится в готовность к использованию. Уточняется план связи, готовится распоряжение по связи и проверяется связь взаимодействия с привлекаемыми (приданными) силами.

Связь в операции организуется, как правило, с помощью подвижного узла связи, к которому организуется радионаправление от узла связи территориального органа.

Связь с подразделениями специального назначения и сводными отрядами организуется по радио, а при возможности – и по полевым кабельным линиям связи. Для обеспечения непрерывной связи к этим подразделениям, как правило, прикомандировываются специалисты связи территориального органа со своими техническими средствами, радиоданными и документами формализованного управления.

В заключение отметим, что для обучения и подготовки сотрудников, в том числе специалистов связи, вопросы организации и обеспечения связи при осложнении оперативных мероприятий, чрезвычайных ситуациях также включаются в планы проведения занятий по служебной подготовке, штабные тренировки и учения.

В зависимости от технического исполнения и решаемых задач средства связи подразделяются на виды.

Так, для управления подвижными нарядами патрульно-постовой службы и осуществления связи с сотрудниками, находящимися в засаде или осуществляющими другие оперативные мероприятия, в том числе с теми, местонахождение которых до момента связи неизвестно, широко используются средства радиосвязи.

В целях циркулярной передачи управляющих команд, контроля работы служебных нарядов, получения осведомительной информации применяются средства телефонной связи.

Быстрая передача текстов документов с автоматическим буквопечатанием и высококачественным документальным оформлением осуществляется с помощью средств телеграфной связи, передача не только текста, но и изображения – средств телефаксной связи. Средства телеграфной и телефаксной связи могут использоваться для ввода и вывода оперативно-служебной информации с помощью ПК.

При необходимости обеспечить качественную и бесперебойную связь по линиям проводной связи используют радиорелейную связь.

Получить визуальную осведомительную информацию с мест наибольшего скопления людей, а также с различных охраняемых объектов позволяет телевизионная связь.

Для громкоговорящего оповещения и персонального вызова используется связь оповещения и персонального вызова.

Лекция 5. СРЕДСТВА И СИСТЕМЫ ТЕЛЕФОННОЙ И РАДИО СВЯЗИ, ПРИМЕНЯЕМЫЕ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

1. Телефонная связь.

2. Радиосвязь.

1. Телефонная связь

Телефонная связь является наиболее распространенным средством передачи информации. Телефонная сеть в настоящее время – это самая развитая коммуникационная система. Она включает в себя каналы связи, аппаратные средства от сельских и ведомственных автоматических телефонных станций (АТС) до междугородных и международных телефонных станций, а также абонентские устройства, среди которых могут быть телефаксы, компьютеры и телефонные аппараты различной степени сложности.

Канал связи – это оснащенные специальным оборудованием физические линии (проводные и оптоволоконные) и радиолинии различного радиуса действия – от сотен метров до нескольких тысяч километров при использовании спутниковых систем.

Базовыми средствами организации телефонной связи являются автоматические телефонные станции. В настоящее время широко используются цифровые АТС. Благодаря наращиваемой архитектуре одна такая станция может удовлетворять потребности не только организаций, но и небольших городов.

Современные базовые АТС представляют собой интегрированные многопортовые платы (на базе микропроцессоров) для аналоговых и цифровых линий. Они, как правило, оснащены несколькими уровнями защиты. Для

защиты от несанкционированного доступа используются либо выделенные телефонные сети, либо волоконно-оптические кабели, с которых затруднен съем информации без специальной аппаратуры.

Самым известным элементом телефонной сети является абонентский телефонный аппарат. Модификаций телефонов в настоящее время очень много: от простейших без номеронабирателя до многофункциональных с большим количеством сервисных функций.

Среди абонентских аппаратов большой популярностью пользуются беспроводные телефоны, радиус действия которых достигает 300 м. Однако во время их работы возникают проблемы электромагнитной совместимости и безопасности, так как переговоры по этим устройствам, как правило, ведутся в открытом эфире и могут легко прослушиваться, иногда с помощью обычных бытовых приемников.

2. Радиосвязь

Мобильная радиосвязь

Первые системы мобильной радиосвязи появились в США в конце 30-х годов и были конвенциональными (радиостанции таких систем работают на закрепленных частотах), предназначенными в первую очередь для полиции и армии и, как правило, одноканальными. В ходе Второй мировой войны появились первые многоканальные системы, однако в них отсутствовали какие-либо средства оптимизации использования каналов: каждой группе абонентов назначался постоянный частотный канал, а переход из одной группы в другую осуществлялся простым переключением частотных каналов. В любой момент могло оказаться, что некоторые каналы не заняты, а другие перегружены. Единственным способом добавления новых групп абонентов к системе было выделение для них дополнительного частотного канала.

Мобильная оперативная радиосвязь – один из важных элементов, обеспечивающих успешную деятельность правоохранительных органов. Основными требованиями к мобильной связи являются:

- оперативность – время на соединение с вызываемым абонентом не должно превышать 0,5–0,8 с;
- простота использования – вызов абонента или группы абонентов с помощью нажатия одной кнопки (тангенты);
- возможность групповой связи, то есть одновременно с несколькими абонентами;
- возможность передачи сигнала тревоги абонентам или диспетчеру (дежурному) нажатием одной кнопки на радиостанции;
- возможность управления связью с пульта дежурного;
- возможность передачи сигнала циркулярного (широкого) оповещения одновременно всем абонентам (радиостанциям);

- возможность передачи короткого текстового сообщения на радиостанцию с дисплеем;
- возможность выхода в телефонную сеть, как служебную, так и общего пользования, непосредственно или через диспетчера;
- высокая надежность, прочность и ремонтпригодность радиостанций;
- высокая помехоустойчивость радиостанций и используемых протоколов связи;
- наличие аппаратуры шифрованной связи с высоким уровнем закрытия, желательно со сменой ключей шифрации по радиоканалу;
- наличие радиостанций скрытого ношения и специальных принадлежностей (гарнитур) для скрытого пользования радиостанциями;
- максимально длительное время работы от одного аккумулятора;
- устойчивость радиостанций к низким и высоким температурам, влажности и иным внешним факторам.

К средствам и аппаратуре мобильной радиосвязи можно отнести собственно портативные, мобильные и стационарные радиостанции, базовые станции и ретрансляторы, служащие для увеличения дальности связи, с соответствующими антенно-фидерными трактами, пультами контроля и управления связью, а также специальные устройства для построения систем связи специального назначения.

Кратко рассмотрим *общие принципы радиосвязи*.

В радиосвязи для передачи информации используются электромагнитные волны, которые распространяются по эфиру и вызываются колебаниями тока (переменным током), текущим по проводнику. Темп, с которым радиосигнал изменяется (колеблется), называется частотой и измеряется в герцах. Большинство используемых частот для радиосвязи измеряются мегагерцами (МГц) – миллионами герц.

Передатчик радиостанции используется для того, чтобы произвести и усилить радиосигнал, который создается путем модуляции голосового сигнала с микрофона. Модулированный и усиленный радиосигнал поступает на *антенну*, излучает его в эфир. Излученный сигнал принимается приемной антенной и поступает на *приемник*. Здесь радиосигнал преобразуется обратно в звуковой и поступает на аудиоусилитель, а затем на динамик радиостанции.

Радиооборудование подразделяется на стационарное, возимое (мобильное) и носимое (портативное).

Стационарное радиооборудование, как правило, размещается в дежурных частях и обычно состоит из стационарной радиостанции, источника питания, антенны и микрофона.

Возимая радиостанция монтируется, например, на автомобиле и предназначена для ведения переговоров как в движении, так и во время остановок.

Носимая портативная радиостанция обладает небольшими габаритами и легко может крепиться на одежде.

Характерными особенностями современных радиостанций являются следующие: профессиональный дизайн, разумное количество органов управления, многофункциональная клавиатура, жидкокристаллический индикатор, позволяющий отображать широкий спектр информации, и большое количество каналов (до 250). Защита передаваемой информации достигается за счет применения скремблеров или шифраторов.

Один из главных параметров радиостанций – ее габаритно-весовые характеристики, которые определяют мощность передатчика и длительность непрерывной работы. Общая тенденция развития радиостанций – их возрастающая интеллектуальность, позволяющая создавать многопользовательские системы с выходом в телефонную сеть общего пользования.

Большинство простых радиосистем являются симплексными, состоящими из радиостанций, работающих на одной частоте. Симплекс означает передачу только в одном направлении в интервал времени на одной частоте.

Ретранслятор – это тип базовой станции, которая служит для обеспечения устойчивой радиосвязи на большей территории. Ретранслятор работает в дуплексном режиме, то есть принимает сигнал на одной частоте и передает на другой одновременно. Радиостанции при этом запрограммированы «наоборот» – первая работает в режиме передачи на частоте приема ретранслятора. Ретранслятор принимает сигнал и одновременно излучает его на своей частоте передачи, которая, в свою очередь, является частотой приема второй станции. Расширение зоны происходит за счет использования в ретрансляторах мощных передатчиков и чувствительных приемников, антенны которых стараются расположить на возвышенностях.

Среди факторов, определяющих зону покрытия, следует выделить:

- *частотный диапазон*. Диапазоны и частоты, на которых разрешена работа в каждом конкретном случае, определяются по согласованию с Государственной комиссией по радиочастотам Российской Федерации и региональным органом внутренних дел;

- *выходную мощность передатчика*, которая обычно не превышает 45 Вт для мобильных станций и 5 Вт – для портативных. Мощность, с которой работает передатчик, регламентируется требованиями региональных отделений Госсвязьнадзора;

- *тип антенны и ее усиление, высоту и положение антенны*. От типа антенны и ее габаритов зависят форма диаграммы излучения и сила сигнала в различных точках местности. Различают направленные антенны, то есть антенны, диаграмма направленности которых вытянута в сторону, и ненаправленные, диаграмма направленности которых имеет форму круга. От высоты поднятия антенны зависит дальность радиосвязи;

- *рельеф территории.* Радиоволны в высокочастотных диапазонах распространяются по прямой линии. И если на их пути имеется препятствие (холм, гора), то за ним образуются участки «затемнения», за которыми радиосвязь невозможна. Высокие здания также являются причиной подобных проблем. Увеличением высоты подъема антенн часто удается устранить такие затемнения;

- *уровень электромагнитных помех.* Причинами сбоев в радиосвязи могут быть не только плохо спроектированные, некачественные средства радиосвязи, но и различные электрические установки и приборы, например, линии электропередачи, неоновые вывески, электродвигатели, генераторы.

Каждый из названных факторов определяет, где возможно установить связь и на каком расстоянии она будет действовать.

В комплект портативной радиостанции должны входить: радиостанция с аккумулятором и антенной; приспособление для крепления на ремень или одежду; запасной аккумулятор; зарядное устройство, выносная гарнитура (необязательно).

Комплект мобильной радиостанции состоит из следующих компонентов: радиостанция с крепежом на автомобиле; выносной микрофон; антенна для крепления на автомобиле (стационарная или магнитная); комплект кабелей для подключения к бортовой сети автомобиля.

При выборе радиостанций следует учитывать различные, иногда внутренне противоречивые, требования: технические характеристики, срок службы, доступность продукта и сервиса, цену и др.

Под техническими характеристиками понимаются: частотный диапазон и сетка частот, поддерживаемые протоколы, излучаемая мощность, количество каналов и функциональные возможности радиостанции. Выбирая радиостанцию, исходят из имеющихся частот или возможности их получения.

Другой критерий – используемые протоколы, которые диктуют функциональные свойства станций. К этим свойствам можно отнести индивидуальный и групповой вызовы, подтверждение доступности станции в зоне связи, индикацию номера вызывающего абонента, дистанционное выключение станции, например, в случае кражи, переадресацию вызова и т.д.

Радиорелейная связь

Радиорелейная связь является разновидностью радиосвязи, организуемой в труднодоступных районах со слаборазвитой первичной сетью и при отсутствии или малой пропускной способности проводных линий связи.

Радиорелейная связь осуществляется в ОВЧ, УВЧ и СВЧ-диапазонах радиоволн. Связь в этих диапазонах практически свободна от атмосферных помех и помех от дальних радиостанций, не зависит от времени года и суток и, следовательно, отличается высокой устойчивостью во времени.

Радиорелейная связь основана на принципе ретрансляции (приема сигналов, их усилении и излучении к следующей станции), осуществляемой с помощью стационарного оборудования и специальных антенн направленного действия, которые могут быть рупорные, параболические и др.

Радиорелейная связь может осуществляться непосредственно между оконечными станциями или через промежуточные радиорелейные станции. Промежуточные станции устанавливаются при необходимости выделения каналов на промежуточных пунктах или значительного расстояния между оконечными станциями, когда непосредственная связь не обеспечивает должного качества.

Принцип действия радиорелейной связи состоит в многократной ретрансляции радиосигналов промежуточными радиостанциями между двумя или более оконечными радиостанциями. Радиорелейные станции имеют специальные устройства многоканального уплотнения. С помощью этих устройств радиорелейные линии связи могут быть уплотнены телефонными и телеграфными каналами связи. Это позволяет транслировать по радиорелейным линиям одновременно телефонные переговоры, телеграфные и даже телевизионные передачи. На этих линиях используется дуплексный способ связи, то есть одновременная передача и прием информации между работающими радиостанциями, причем прием и передача осуществляются на разных частотах.

При организации радиорелейной связи оконечные и промежуточные радиостанции устанавливаются с расчетом обеспечения прямой видимости антенн между предыдущей и последующей радиостанциями. В самом общем виде радиорелейную линию связи можно представить как цепочку приемопередающих радиостанций.

При выборе трасс радиорелейных линий учитывается рельеф местности. В среднем при высоте антенны 70–80 м расстояние между двумя радиостанциями радиорелейной линии составляет 40–60 км. При установке радиостанций на горах или больших возвышенностях расстояние между станциями значительно увеличивается и может достигать 100–150 км.

Транкинговая радиосвязь

Термин «транкинг» происходит от английского слова trunking – объединение в пучок. Этот термин пришел из телефонии, где давно используется принцип предоставления абоненту свободного в данный момент канала связи.

Транкинг – это автоматическое динамическое распределение каналов между абонентами. При этом нет жесткого закрепления абонентов за каналами связи – все каналы находятся в общем пользовании и предоставляются абонентам по мере поступления запросов. Это позволяет избежать перегрузки одного канала, в то время как соседний канал не будет востребован. Для управления

распределением каналов к традиционным базовым станциям добавляется специальное устройство – контроллер.

Динамическое распределение ограниченного количества каналов связи большого числа пользователей и управление доступом к свободным каналам осуществляет транкинговая система, а не пользователь. Как и в телефонной сети, абонент может указать конечный пункт, но не маршрут, по которому будет произведено соединение.

Зона радиопокрытия транкинговой системы зависит от организации инфраструктуры (числа базовых станций и репитеров) и технических возможностей контроллера.

Принцип действия транкинговой связи заключается в следующем. Радиостанция, с помощью которой вызывается другая радиостанция или группа радиостанций, абонент телефонных сетей общего пользования и т. д., посылает по радиоканалу на контроллер пакет данных. Это может быть выделенный радиоканал, называемый контрольным, или обычный разговорный канал. В пакете содержится идентификатор радиостанции, запрос на предоставление канала и идентификатор вызываемой стороны. Контроллер, получив такой пакет, проверяет наличие в системе радиостанции вызываемого корреспондента (при включении радиостанции она регистрируется – посылает свой идентификатор контроллеру), ищет свободный канал, направляет вызывающей и вызываемой радиостанциям команду перехода на свободный канал, после чего обрабатывает следующий вызов. Этот процесс в зависимости от конфигурации системы занимает от 300 миллисекунд до нескольких секунд.

Транкинговые системы предоставляют следующие возможности: групповой вызов, персональный внутренний вызов, приоритетные вызовы, доступ к телефонным сетям общего пользования.

Конвенциональная радиосвязь

Конвенциональная система связи обычно включает в себя портативные и мобильные радиостанции, иногда – ретранслятор для увеличения дальности связи. Во время прямой связи между радиостанциями они могут работать в симплексном режиме (одна частота для приема, передачи) или в полусимплексном (две частоты: одна для приема, другая – для передачи сообщений). Второй режим иногда называют «двухчастотный симплекс». В случае использования ретранслятора необходимо работать в полудуплексном режиме.

В качестве ретрансляторов в конвенциональных системах часто используют устройства, скомпонованные на базе двух мобильных радиостанций. Такие ретрансляторы относительно просты и недороги, но имеют существенные недостатки, а именно: ограниченную выходную мощность и невозможность работать в непрерывном режиме, а также быть объединенными на одно антенно-фидерное устройство. Для построения многоканальной компактной зоны связи с

одной антенной необходимо применять специально разработанные для подобных целей ретрансляторы, которые впоследствии могут быть использованы для построения транкинговых систем.

В настоящее время известны несколько цифровых стандартов построения таких систем. Так, например, стандарт АПКО-25 предусматривает совместимость с обычными аналоговыми радиостанциями, парк которых в правоохранительных органах очень велик.

Радиотелефонные сотовые сети

Архитектура сотовых радиотелефонных сетей основана на принципе деления определенной территории на участки (соты), в каждом из которых действует радиостанция с ретранслятором. Все они связаны с центральной станцией, имеющей выход на городскую телефонную сеть. Абонент, перемещаясь в зоне действия сети, «передается» от одной периферийной станции к другой с динамическим изменением канала связи.

Развитие сотовой связи знаменует переход на цифровую организацию каналов. Сокращение размеров сот влечет уменьшение размеров радиотелефонов и увеличение их ресурсов, эффективное использование частотного диапазона. Использование более высоких частот позволяет уменьшить влияние промышленных помех и разгрузить эфир. К сотовому телефону можно подключить модем, что дает, например, возможность пользоваться переносными компьютерами для передачи и приема факсимильных сообщений и данных по электронной почте.

В отличие от систем конвенциональной и транкинговой радиосвязи мобильная телефонная (сотовая) связь предназначена в первую очередь для обеспечения персональной мобильной голосовой связи «один на один». Технологии сотовой связи прошли примерно тот же путь развития, что и транкинговые системы. Все аналоговые стандарты сотовой связи обеспечивают хорошее качество передачи голоса. Их основным недостатком, как и в случае с аналоговыми транкинговыми системами, является ограниченная емкость. Кроме того, в аналоговых системах сотовой связи сохраняется проблема защиты от несанкционированного доступа к системе.

В начале 90-х годов повсеместно начался переход на цифровые стандарты сотовой связи. Большое распространение получил западноевропейский стандарт GSM, принятый в настоящее время более чем в ста странах.

Следует отметить, что в мобильной телефонной связи цифровые технологии далеко не всегда обеспечивают более высокое качество звука по сравнению с аналоговыми системами. Основные преимущества цифровых стандартов мобильной телефонной связи – большая емкость системы, конфиденциальность переговоров и устойчивость к различного рода радиопомехам. И цифровые, и большинство аналоговых стандартов мобильной телефонной связи также предоставляют возможность передачи текстовых сообщений и данных.

Сотовая связь имеет свойства, отличающие ее от других видов мобильной связи. К ним относятся:

- многократное использование радиоканалов в системе для увеличения количества обслуживаемых абонентов на одной и той же территории без расширения занимаемого спектра частот;
- полный набор функций проводной телефонной связи, включая выход на междугородную и международную сети;
- возможность для абонента вести телефонные переговоры на всей территории обслуживания компании-оператора сотовой связи;
- перемещение абонента по всей зоне обслуживания без прерывания разговора, что обеспечивается автоматическим переключением соединения от одной базовой станции к другой.

Немаловажны для пользователей сотовой связи и такие ее услуги, как длительная непрерывная работа без подзарядки аккумуляторов, практическое отсутствие неблагоприятного воздействия на потребителя, высокая защита от прослушивания и нелегального использования номера, а также передача данных, факсов, коротких сообщений, голосовая почта, автоматическое определение номера и др.

Системы персонального радиовызова

Системы персонального радиовызова предназначены для оперативной передачи коротких сообщений или сигналов на малогабаритные приемники. Радиус действия может охватывать значительные территории. Передача осуществляется с центрального пульта, имеющего мощный передатчик.

Системы персональной тревожной сигнализации

Системы персональной тревожной сигнализации обеспечивают передачу сигнала, кодируемого личным шифром абонента, на центральный диспетчерский пульт. Передатчик может быть выполнен в виде наручных часов.

Пейджинговая связь

Пейджинговая связь, так же как система персонального радиовызова, не дает возможности двухстороннего обмена информацией, но сохраняет все преимущества указанной системы. Отличие от системы персонального радиовызова заключается в использовании инфраструктуры телефонной сети, то есть качественно иного коммуникационного уровня.

Рассмотрим некоторые разновидности пейджеров.

Текстовый пейджер представляет собой приемник буквенно-цифровых текстовых сообщений. В зависимости от модели позволяет хранить сообщения определенное время и при смене питания, производить подключение к персональному компьютеру, становиться составной частью охранных систем и т. д.

Твейджер – приемопередающий пейджер. Он может и получать сообщение, и подтверждать его получение адресатом. В нем запрограммированы стандартные сообщения – для ответа пользователь нажимает нужную кнопку. Кроме того, он дает возможность набрать текст в виде цифр и знаков и отправить его на пейджеры, твейджеры, электронную почту либо передать в виде голосового сообщения на обычный или сотовый телефон.

Если адресат получает сообщение на обычный или сотовый телефон, то оно представляет собой синтезированное голосовое сообщение, воспроизводимое системой компьютерной телефонии с помощью факс-модемной специализированной платы с функцией «текст-голос».

Графический пейджинг позволяет сетевым операторам пейджинговой связи передавать высококачественные графические изображения абонентам: субъективные портреты преступников для опознания, сканированные факсы, карты с маршрутами движения и т. д. Воспроизводятся изображения на экране пейджера с использованием 8 строк по 26 символов. Имеется возможность хранения сообщений, которые не были приняты из-за перегрузки или уничтожены после прочтения (сообщения после просмотра можно хранить в виде отдельных файлов и использовать в дальнейшем). В большинстве моделей предусмотрены «телефонный справочник» с указанием номеров телефонов и фамилий, «перечень неотложных дел» и «напоминающих событий», подающих сигнал в установленное время. Можно изменить масштаб текстового сообщения и просмотреть его в укрупненном виде.

Голосовой пейджинг – компромиссная технология, предоставляющая три разновидности сервиса:

1. Звонящие абоненту пользуются услугами оператор-ской службы. Оператор вводит номер абонента, после чего система записывает голос удаленного абонента и пересылает его в эфир на голосовой пейджер.

2. Нет операторской службы, и ввод номера абонента осуществляется тоном – с помощью телефонного аппарата с поддержкой тонального набора или обычного аппарата с биппером (брелоком с цифровой клавиатурой) и обтюратором, прикладываемым к телефонной трубке.

3. Компания-оператор передает абоненту голосового пейджера специальный модернизированный цифровой автоответчик, который может быть установлен на любом доступном для абонента номере телефона, который «отвечает» на входящие телефонные звонки и пересылает все надиктованные на него сообщения прямо на терминал пользователя.

Криптопейджер – абонентское устройство в криптозащищенной системе пейджинговой связи. Сервер криптозащиты должен проходить обязательное лицензирование в ФСБ России. Абоненты такой пейджинговой системы имеют возможность выхода на операторский центр по каналам спецсвязи, а также линиям телефонной сети с использованием скремблеров. При необходимости индивидуальный ключ абонента может быть оперативно автоматически изменен

при получении новой информации, что исключает вероятность прочтения сообщений при перехвате.

Безэкранный пейджер – возможность принимать большие объемы информации и вводить их в персональный компьютер. Пейджер присоединяется к компьютеру, когда заполняется весь объем его оперативной памяти.

Оценки экспертов показывают, что даже при значительном удешевлении услуг сотовой связи мобильный телефон не вытеснит пейджер, так как пейджерная связь обходится пользователю в 8–10 раз дешевле сотовой. Таким образом, пейджерная связь – неотъемлемая часть инфраструктуры современного общества.

Системы спутниковой связи

В настоящее время интенсивно развиваются космические технологии в области спутниковой связи, передачи данных и вещания. Эта область составляет 75 % общего объема мирового рынка космических технологий. На геостационарных орбитах действуют примерно 185 космических спутников связи и вещания. Современные спутниковые системы связи по пропускной способности соизмеримы с волоконно-оптическими линиями связи, однако их стоимость намного выше.

Термин «системы универсальной подвижной спутниковой связи» предусматривает интеграцию наземных сотовых сетей, спутниковых систем и расширение услуг связи. В связи с большим ростом информационных потребностей спутниковые каналы развиваются так же интенсивно, как и наземные системы на базе волоконно-оптических линий. Внедрение многолучевых антенных систем в сочетании с современными усилителями мощности сигнала позволили создать высокоэнергетические спутниковые каналы, работающие с терминалами малых систем.

Международный регламент радиосвязи классифицирует спутниковые службы связи следующим образом:

- фиксированные службы (связь между наземными станциями, расположенными в строго определенных пунктах);
- подвижные службы (связь между мобильными объектами – судами, самолетами, автомобилями и т. д.);
- радиовещательные службы (непосредственное и распределительное телевидение).

Отметим, что к основным достоинствам спутниковой связи относятся: обширная зона покрытия; высокое качество и надежность связи; независимость стоимости передачи информации от расстояния и количества точек приема; быстрое развертывание в малоосвоенных местностях; гибкая конфигурация. Вместе с тем к основным недостаткам этой системы связи можно отнести: более высокую, чем в наземных сетях, стоимость передачи единицы информации через спутник из-за ограниченности ресурса спектра частот; возникновение трудноразрешимых вопросов, связанных с национальными законодательствами

и высокими ценами на услуги лицензирования; определенный риск использования спутниковых технологий в связи с большим количеством отказов по различным причинам, которые могут быть как технологического, так и естественного происхождения.

В настоящее время для обеспечения подвижной телефонной связи используются различные системы (INMARSAT, GLOBALSTAR, IRIDIUM и др.).

Так, глобальная низкоорбитальная система IRIDIUM, не являясь в буквальном смысле системой оперативной связи, оказалась незаменимой для правоохранительных органов, которым по роду своей деятельности нужна связь на больших территориях, не охваченных радиопокрытием других систем, специального назначения или сотовых. Она по возможностям и функциям ближе к сотовым системам. Абонентские радиостанции этой системы невелики по размерам и не требуют точного позиционирования антенн по отношению к спутнику, как в других системах спутниковой связи, поэтому могут работать даже в движении и в ряде случаев являться единственным средством оперативной связи.

В системах спутниковой связи предусмотрено оказание и услуг пейджинговой связи (спутниковый пейджинг). Предоставляются следующие виды услуг пейджинговой связи:

- передача алфавитно-цифровых сообщений – при этом абонент предварительно обязательно указывает до трех зон (территория России условно поделена на 18 зон), куда для него могут передаваться сообщения;
- глобальное оповещение для осуществления глобального пейджинга, которое основывается на данных о последнем местоположении пользователя.

В спутниковой сети связи существуют три типа пейджеров: тональные, цифровые, текстовые, а также их модификации.

Комплексы слежения и пеленгации

Комплексы слежения и пеленгации предназначены для постоянного контроля за местоположением мобильных объектов. В настоящее время существует два класса систем слежения: наземные и космические.

К *наземным системам* относятся средства контроля за перемещением мобильных объектов и средства пеленгации, определяющие координаты любого передатчика.

Пеленгуя при помощи специальных антенн с каждой базовой станции слежения радиопередатчик, установленный, например, на транспортном средстве, можно получить информацию о направлении и скорости перемещения объекта. Каждый объект может иметь свой идентификационный код. В этом случае автоматические станции слежения, опрашивая кодовые датчики, отмечают на электронной карте местоположение мобильных объектов. Погрешность определения координат не превышает 100 м.

Космические системы слежения разделяются на два типа. Первый тип связан с применением на мобильных объектах приемников, работающих в системе GPS NAVISTAR (Global Position System). Эта спутниковая национальная система открыта для широкого использования.

Вторая космическая система пеленгует на орбите сигнал, поступающий от радиомаяков, установленных на каждом транспортном средстве. При этом спутник сначала накапливает информацию, затем в определенной точке орбиты передает в наземный центр обработки данных. В итоге время доставки информации несколько увеличивается.

Так, спутниковая навигационная система GPS NAVISTAR обеспечивает:

- непрерывный контроль за транспортными средствами;
- отображение координат, маршрута и скорости движения объекта на электронной карте диспетчера;
- оперативное реагирование на внештатные ситуации;
- оптимизацию маршрутов и графиков движения.

Приемники системы осуществляют непрерывную, глобальную и всепогодную навигацию с точностью определения координат и высоты над уровнем моря до 100 м, а в дифференцированном режиме – до 5 м.

Коротковолновая связь

В КВ-диапазоне (2–30 МГц) коротковолновая связь осуществляется пространственными ионосферными волнами с дальностью до нескольких тысяч километров.

Системы коротковолновой связи применяются для передачи данных, факсов, голосовой связи и автоматической телефонной связи в любую точку планеты.

Отметим, что в этой системе связи обеспечивается возможность подключения УКВ-оборудования в коротковолновую сеть с географическим разделением передачи и приема.

Таким образом, с учетом изложенного системы мобильной радиосвязи можно разделить на две большие группы: конвенциональные и транкинговые, причем каждая из групп может включать в себя как аналоговые, так и цифровые или цифроаналоговые средства связи.

В конвенциональных системах за пользователем радиостанцией обычно закреплен один или несколько вручную переключаемых частотных каналов. Простейшим вариантом здесь является случай, когда все радиостанции, запрограммированные на данный канал, «слышат» друг друга, то есть являются одной разговорной группой. Тем не менее дальнейшее развитие конвенциональных средств привело к появлению «протоколов сигнализаций», когда одновременно с речью по эфиру передается специальная кодовая информация, позволяющая осуществлять индивидуальный и групповой вызов соответствующих абонентов. Как правило, конвенциональные системы до последнего времени являлись однозоновыми, обеспечивающими радиосвязь в

пределах одной базовой станции, которая осуществлялась только через оператора связи (диспетчера) с помощью стационарной радиостанции. Применяемая в настоящее время аппаратура позволяет преодолевать эти ограничения и создавать конвенциональные системы с широким радиопокрытием.

В транкинговых системах абоненту при нажатии тангенты автоматически выделяется свободный частотный канал из набора частот всей системы. Это позволяет более эффективно использовать частотный ресурс системы, увеличить число абонентов на частотный канал и повысить надежность связи, например, при отказе ретранслятора, поскольку в любом случае канал связи будет предоставлен, если, конечно, есть свободный и исправный. Тем не менее реально эффективность транкинговых систем проявляется, если частотных каналов не менее трех, а число абонентов свыше 100–200.

Лекция 6. СПЕЦИАЛЬНАЯ ТЕХНИКА КАК СРЕДСТВО ДОБЫВАНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИИ

- 1. Понятие информации правоохранительных органов.***
- 2. Понятие оперативно-розыскной информации.***
- 3. Роль специальной техники в получении оперативно-розыскной информации.***

1. Понятие информации правоохранительных органов

Для эффективного выполнения задач борьбы с преступностью правоохранительные органы проводят комплекс мероприятий, результаты которых в значительной степени зависят от умелого и грамотного применения различных технических средств. Правильное использование специальных технических средств позволяет выявить признаки готовящихся или скрытно совершаемых преступлений, документировать факты преступных проявлений, создать базу для расследования преступлений, обеспечить условия защиты людей в криминальных ситуациях.

Технические средства позволяют не только гласно и негласно получить оперативную информацию и осуществить ее фиксацию, но и обеспечить дальнейшую передачу по различным каналам связи в автоматизированный банк данных, осуществляя в рамках законности накопление необходимых сведений

для последующей аналитической обработки, в том числе по специальным компьютерным программам.

Информация, зафиксированная на материальном носителе, позволяет на стадии предварительного следствия или судебного рассмотрения дела в случае необходимости не только однозначно установить ее источник, но и убедительно доказать ее достоверность, обоснованность и объективность. Она может быть подвергнута проверке на аутентичность в ходе следственных или судебных действий, а материальный носитель передан для проведения соответствующей судебной экспертизы.

Таким образом, с появлением новых информационных технологий, основанных на широком внедрении средств вычислительной техники, связи, систем телекоммуникаций, информация становится постоянным и необходимым атрибутом обеспечения деятельности государства, юридических лиц, общественных объединений и граждан. От ее качества и достоверности, оперативности получения зависят многие решения, принимаемые на самых разных уровнях – от главы государства до гражданина. Информация – это основной объект информационного общества, и ее роль трудно переоценить. Отражая реальную действительность, она пронизывает все направления деятельности, общества в целом и каждого человека в отдельности.

До середины XX века под информацией понимались «сообщения и сведения», передаваемые людьми устным, письменным или иным способом. С середины XX века информация превращается в общенаучное понятие, включающее в себя обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму.

Простое и понятное каждому определение информации дал С.И. Ожегов: «Информация – 1) сведения об окружающем мире и протекающих в нем процессах, воспринимаемых человеком или специальными устройствами; 2) сообщения, осведомляющие о положении дел, о состоянии чего-нибудь».

Информационное воздействие на государство, общество, гражданина в настоящее время более эффективно и экономично, чем политическое, экономическое и даже военное. Информация становится реальной, почти физически ощутимой силой. В современном обществе информация играет решающую роль, а информационные ресурсы становятся в один ряд с важнейшими ресурсами государства – природными, трудовыми, финансовыми и иными, составляющими его потенциал.

Появление электронно-вычислительных машин, их широкое использование в повседневной человеческой деятельности сравнимо по значению с двумя величайшими техническими свершениями: овладением огнем и силой пара. Каждое из них, как известно, явилось переворотом в жизни людей.

В основе производства, распространения, преобразования и потребления информации лежат информационные процессы создания, сбора, обработки,

накопления, хранения, поиска, получения, распространения и потребления информации, а также процессы создания и применения информационных систем, информационных технологий и средств их обеспечения, средств и механизмов информационной безопасности данной системы. Общественные отношения, подлежащие правовому регулированию, возникают при выполнении именно этих информационных процессов и называются информационными, а деятельность по осуществлению информационных процессов – информационной. Таким образом, основным объектом правоотношений в информационной сфере деятельности является информация.

В Федеральном законе от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» определяет информацию как любые сведения независимо от формы их представления.

Следует отметить, что к документированной информации можно отнести зафиксированную на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать. Понятие «документированная информация» основано на двуединстве: информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений. Информация «закрепляется» на материальном носителе или даже «привязывается» к нему и таким путем обособляется от своего создателя.

Применение современных информационных технологий вызвало и негативные последствия – появление новых видов преступлений (например, компьютерных), ранее не известных праву, основанных, прежде всего, на возможностях несанкционированного и неправомерного доступа к информации.

Информация имеет свои источники. Информационный источник – любая система, вырабатывающая сообщения или содержащая информацию, предназначенную для передачи. По форме представления различают следующие виды источников информации:

- текстовые – книга, журнал, рукопись и т. д.;
- графические, или изобразительные, – график, чертеж, план, карта и др.;
- аудиовизуальные – звукозапись, кинофильм, диапозитив и иные источники.

Информацию можно делить на виды в зависимости от сферы возникновения, способа передачи, а также назначения. Принято различать три вида информации в зависимости от сферы ее возникновения:

- элементарная – неживая природа;
- биологическая – мир животных и растений;
- социальная – человеческое общество.

Кроме того, информацию условно делят на эстетическую и семантическую.

Эстетическая информация обязана своим происхождением возникающим в природе различным сочетаниям звуков, запахов, света, цвета и теней. К

эстетической информации относят различные произведения искусства (музыкальные, художественные, литературные).

Семантическая информация возникает в результате различной деятельности людей. В правоохранительной сфере семантической информацией может быть сообщение о совершенном преступлении. Информация, собранная на месте преступления, также является семантической. Она – результат криминалистической деятельности работников правоохранительных органов.

В зависимости от способа передачи и восприятия можно выделить следующие виды информации:

- визуальная – передается и воспринимается визуальными образами;
- аудиальная – передается звуками;
- тактильная – передается ощущениями;
- одорологическая – передается запахами;
- машинно-ориентированная – воспринимается и обрабатывается на ЭВМ.

К наиболее часто встречающимся характеристикам информации относятся: целевое назначение, объем, ценность, полнота, надежность, достоверность, избыточность, скорость передачи и обработки информации.

Всю информацию с позиций информационного права по формам доступа можно разделить на две группы: открытую, свободно распространяемую в информационной сфере, и ограниченного доступа, распространение которой возможно только в условиях конфиденциальности или секретности.

Рассматривая информационное обеспечение правоохранительных органов, прежде всего необходимо остановиться на учетах, которые используются для регистрации первичной информации о преступлениях и лицах, их совершивших.

Учеты правоохранительных органов подразделяются на оперативно-справочные, криминалистические и розыскные. Объектами учетов являются определенные категории лиц, событий, предметов.

2. Понятие оперативно-розыскной информации.

Оперативно-розыскная информация - это получаемые субъектом оперативно-розыскной деятельности с помощью специальных методов и средств фактические данные, содержащие в себе знания, необходимые и пригодные для предотвращения и раскрытия преступлений, розыскной работы и решения иных задач борьбы с преступностью. Оперативно-розыскная информация является разновидностью социальной информации, специфичной по цели получения (борьба с преступностью), методам получения и режиму использования, обеспечивающему конспирацию, надежную зашифровку источников, возможность проверки сообщаемых сведений и их применение только заинтересованными работниками¹.

¹ См. Волчков И.М. Оперативно-розыскная информация: сущность и методология ее реализации: Учеб.пособие. – Псков, 2002, Оперативно-розыскная деятельность: Учебник /

Анализ литературы показывает, что содержание оперативно-розыскной информации характеризуется широким разнообразием сведений, относящихся также к характеристике оперативной обстановки, основных сил, средств и методов оперативной деятельности, оценке результатов их использования¹. Оперативно-розыскная информация, являясь производной от оперативно-розыскной деятельности, обладает присущим только ей чертами: спецификой данных, подлежащих поиску, сбору, переработке и использованию; особенностями источников возникновения; спецификой её прохождения от источников к потребителю; особенностями её обработки, использования и правового регулирования; спецификой субъекта получения; способностью объективно отражать реальные факты, явления (процессы), обстоятельства, имеющие значение для борьбы с преступностью.

С точки зрения познавательного назначения используемую в оперативно-розыскной деятельности информацию классифицирует по пяти основным направлениям:

- изучение оперативной обстановки;
- исследование конкретных обстоятельств, требующих мер предотвращения преступления;
- установление обстоятельств совершенного преступления и получение данных о доказательствах;
- установление обстоятельств побега из-под стражи или уклонения от следствия, суда и получения данных о месте нахождения виновных;
- обеспечение тактики предотвращения и раскрытия преступлений.²

Оперативно-розыскная информация разделяется в зависимости от её соотношения с целями и решаемыми задачами ОРД на стратегическую и тактическую.

Стратегическая информация определяет цели и содержание процессов управления оперативно-розыскной деятельности. На её основе избираются перспективные направления развития оперативно-розыскной деятельности, определяются наиболее важные цели, устанавливается их иерархия, последовательность, пути и средства достижения. Такая информация позволяет заранее предвидеть отклонения системы от заданной цели и в соответствии с этим повышать степень приспособляемости системы оперативно-розыскной деятельности к изменяющейся с течением времени социальной среде. Стратегическая информация содержит вероятную (прогностическую) картину отдаленного процесса и потому является одной из основ стратегических планов.

Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Сенилова, А.Ю. Шумилова. – М.: Инфра-М, 2004., с.654.

¹ Овчинский С.С.. Оперативно-розыскная информация. \Под ред. А.С. Овчинского и В.С. Овчинского. М.: ИНФРА – М, 2000. с.40-62.

² Овчинский С.С. Указ. работа, с.43-44.

Стратегическая информация создает предпосылки для успешного решения тактических задач оперативно-розыскной деятельности. Имея общее представление о состоянии и тенденции развития преступности в конкретных регионах (по линиям работы оперативных аппаратов), руководители и работники оперативных аппаратов смогут принимать успешные решения по конкретным делам оперативно-розыскного учета и материалам как в рамках оперативно-тактического планирования, так и в проведении конкретных оперативно-розыскных мероприятий.

Практическое значение разделения оперативно-розыскной информации на стратегическую и тактическую состоит в обеспечении полного удовлетворения информационных потребностей оперативно-розыскной деятельности в борьбе с преступностью.

По своему содержанию оперативно-розыскная информация представляет собой сведения об определенной группе объектов, к которым относятся, во-первых, лица; во-вторых, факты (события); в-третьих, предметы (вещи); в-четвертых, места, представляющие в той или иной степени оперативный интерес, отражение которых в сознании оперативных работников обуславливает возникновение данной информации.

Источниками получения тактической оперативно-розыскной информации сотрудниками оперативных аппаратов могут быть, прежде всего, различные граждане, с которыми оперативные работники вступают в контакт. Их разделяют на:

- законопослушных граждан;
- маргинальных лиц, которые соприкасаются с преступным миром, но не являются в принципе, его атрибутивным элементом;
- преступников, занимающихся совершением общеуголовных, насильственных, корыстных и корыстно-насильственных преступлений в составе групп, как правило, с неустойчивой структурой и в одиночку;
- организаторов и членов организованных преступных групп, в том числе мафиозного и профессионального типа, для которых устойчивая противоправная деятельность обычно является основным источником существования.

В соответствии с количественной и качественной неоднородностью выше перечисленных категорий лиц определяются и реализуются задачи оперативных аппаратов по обнаружению, сбору, фиксации, закреплению, сохранению оперативно-розыскной информации для последующей её эффективной реализации в целях борьбы с преступностью.

В процессе функционирования оперативные аппараты постоянно взаимодействуют с законопослушными гражданами как источниками информации, необходимой для выявления, предупреждения, раскрытия преступлений и розыска скрывшихся преступников с одной стороны, с другой стороны, их отношения (экономические, политические, социальные,

нравственные и т.д.) являются объектом посягательства преступников, и некоторые из них под влиянием криминальных факторов изменяют свое поведение с законопослушного на маргинальное (находящееся на грани преступного поведения) или противоправное. Поэтому, являясь носителем такой информации, они должны оставаться в свою очередь в сфере профилактического воздействия со стороны органов внутренних дел вообще и оперативных аппаратов в частности.

Маргинальная группа граждан - это бродяги, проститутки, наркоманы, алкоголики и пр., как правило, постоянно соприкасаются с преступным миром, при определенных условиях они могут встать на путь совершения преступлений. В этой связи эта категория лиц как источник оперативно-розыскной информации является для оперативных аппаратов весьма существенной.

Категория общеуголовных преступников по своей численности в общем составе всех преступников занимает абсолютное большинство. Информация о замышляемых преступлениях данной категории лиц представляют значительный оперативный интерес.

Устойчивая противоправная деятельность характерна для преступников мафиозного и профессионального типа. Численность этих представителей преступного мира незначительна, но их общественная опасность исключительно велика. Именно эта категория преступников широко использует в своей деятельности для обеспечения успеха и безопасности тайные методы, включая разведку и контрнаблюдение. Это обстоятельство крайне важно учитывать оперативным аппаратом при организации разведывательной работы в этой устойчивой преступной среде.

К особой категории источников оперативно-розыскной информации относятся лица, оказывающие конфиденциальное содействие оперативным подразделениям.

Таким образом, с учетом выше названных литературных источников, оперативно-розыскную информацию можно рассматривать как фактические данные, полученные субъектом системы оперативно-розыскной деятельности посредством управления её силами, средствами и методами, объем и содержание которых устраняет неопределенность и обеспечивает функционирование данной системы в решении стоящих перед оперативными аппаратами задач в борьбе с преступностью.

3. Роль специальной техники в получении оперативно-розыскной информации

Одним из мощнейших средств получения оперативно-розыскной информации является специальная техника оперативно-розыскного назначения,

которая представляет собой совокупность технических средств и научно обоснованных специальных приемов их правомерного применения оперативными аппаратами в процессе осуществления оперативно-розыскных мероприятий. Эта техника применяется в сфере оперативно-розыскной деятельности оперативными работниками или другими лицами по их указанию, как правило, негласно, в целях решения задач, возложенных на оперативно-розыскную деятельность и определенных законом.

Говоря о социальной обоснованности использования технических средств¹ при сборе оперативно-розыскной информации, следует отметить, что тенденции развития оперативно-розыскной деятельности таковы, что она все в большей мере становится наукоемкой, опирается на возможности современных информационных технологий и, в первую очередь, на применение специальных технических средств контроля, фиксации и обработки информации. Оперативные подразделения правоохранительных органов имеют длительную историю применения самых разнообразных технических средств для решения специфических задач предупреждения и раскрытия преступлений, розыска скрывающихся преступников.

В то же время применение наиболее наукоемких технических средств разведывательного назначения многие годы было прерогативой военных ведомств и спецслужб. Лишь в начале 90-х годов пришло осознание того обстоятельства, что организованная преступность представляет собой настолько мощное и социально опасное явление, что оно достойно применения в борьбе с ним всех средств и методов, которые применяются против вражеских армий и государств. В силу этого в арсенале технических средств особое место заняла специальная техника оперативно-розыскного назначения. Она выступает эффективным инструментом ОРД и используется для скрытого документирования преступных действий или скрытого получения информации, т.е. действий, которые осуществить иным путем невозможно либо нецелесообразно.

Научно-технические достижения последних лет стали основой создания широкого спектра технических средств разведывательного назначения нового поколения, обладающих мощными тактическими возможностями по сбору оперативно-розыскной информации: скрытый электронный контроль передвижения объектов в сложных городских условиях; скрытый акустически и контроль помещений без размещения в них какой-либо аппаратуры; контроль психофизиологического состояния человека. При этом миниатюризация технических средств, применение цифровых методов обработки данных, новых физических принципов действия не только повышают эффективность решения

¹ При подготовке данного параграфа использовалось открытое издание: Оперативно-розыскная деятельность: Учебник / Под ред. К.К.Горяинова, В.С.Овчинского, Г.К.Синилова, А.Ю. Шумилова. – М.: Инфра-М, 2004. С.388-403.

традиционных задач, но и позволяют реализовать принципиально новые, недоступные ранее технологические схемы скрытого добывания информации. Соответственно развивается и усложняется тактика применения специальной техники в ОРД.

Принципиально новое обстоятельство, которое необходимо учитывать, подходя к тактике применения технических средств при сборе оперативно-розыскной информации заключается в том, что отказ от государственной монополии в сфере оборота специальной техники породил проблему ее нелегального распространения и использования. В немалой степени этому также способствовали и произошедшие социально-экономические преобразования, и явное несовершенство соответствующей нормативно-правовой базы.

Оперативные подразделения правоохранительных органов регулярно выявляют факты нелегального оборота и применения специальной техники. С начала 90-х годов число зарегистрированных случаев нелегальной работы в сетях связи органов внутренних дел, федеральной службы безопасности, министерства обороны увеличилось в тысячи раз. Выборочный анализ состояния оперативной обстановки по ряду регионов России (в первую очередь, с высокой плотностью населения и развитыми экономическими инфраструктурами) позволяет выявить устойчивую тенденцию повышения технической оснащенности криминальных структур, и прежде всего организованных преступных формирований. Причем, рост технической «вооруженности» происходит в основном за счет радиоэлектронной аппаратуры разведывательного назначения и технических средств организации, подготовки и совершения конкретных видов преступлений.

Наличие подобного арсенала техники, характеристики которой часто превосходят соответствующий уровень субъектов ОРД, позволяет осуществлять разведывательные и контрразведывательные акции в отношении правоохранительных органов, акты промышленного шпионажа, другие преступления в сфере высоких технологий.

Еще одним фактором, оказывающим мощное воздействие на современную тактику ОРД, тактику применения специальной техники оперативно-розыскного назначения, является возникновение и бурное развитие в нашей стране рынка технических средств защиты информации, в том числе электронного противодействия. Сотни фирм предлагают в настоящее время целый спектр импортной и отечественной техники защиты: от простейших индикаторов несанкционированного подключения к телефонным линиям до сложных компьютерных комплексов непрерывного радиомониторинга и современных систем охранного телевидения, сигнализации и управления доступом.

Развитие специальной техники оперативно-розыскного назначения и защиты информации вызывает необходимость анализа рынка существующих и перспективных моделей технических средств. Любое совершенствование или изобретение нового метода или средства разведки (защиты) закономерно

приводит к созданию соответствующего метода или средства защиты (разведки).

Анализ практики свидетельствует о том, что повышение замаскированности и профессионализма действий преступников в современный период, появление новых видов преступлений требуют адекватных мер противодействия. Совершенно очевидно, что числе таких мер наибольший эффект дает в совокупности целенаправленное техническое проникновение в преступную среду. Особо актуально техническое противодействие организованной преступности. Это обусловлено высокой технической оснащенностью криминалитета. Так, из общего числа разоблаченных организованных преступных формирований более половины использовали технические средства. Количество преступных посягательств, совершенных с использованием технических средств постоянно увеличивается. Характерно то, что применяемые преступниками технические средства разнообразны по содержанию и практически все находятся на современном уровне. Организованные преступные группы активно используют новейшие средства связи, приборы видения в темноте, оптические прицелы, устройства звукозаписи, телефоны с определителем номера, электронные записные книжки, радиотелефоны, технические средства защиты информации. Криминалитет активно изучает новую специальную технику, посещает соответствующие выставки. Преступные группировки используют значительные средства для приобретения такой техники. Это требует со стороны оперативных подразделений адекватного технического вооружения.

Кроме того, отмечается высокая конспиративность действий организованных преступных групп, активное противодействие оперативным аппаратам в процессе сбора ими оперативно-розыскной информации. Учитывая эти меры противодействия со стороны преступной среды, следует признать, что использование технических средств и методов оказывается для субъектов ОРД во многих случаях единственным средством сбора, поступления необходимой оперативно-розыскной информации.

Анализ перечня оперативно-розыскных мероприятий позволяет говорить о том, что эффективность их проведения, получение требуемой информации во многом определяется использованием при этом соответствующих технических средств.

Так, в большинстве случаев опроса обычно используют технические средства аудио- и видеозаписи. Это обусловлено тем, что по ряду причин опрашиваемый в дальнейшем может отказаться от даваемой первоначально информации.

При наведении справок в отношении организованных преступных формирований довольно часто возникает опасность в утрате или фальсификации, а иногда и в полной замене различных документов, содержащих важную оперативно-розыскную розыскную или доказательственную информацию. Если такой опасности и не возникает, то

никто не может гарантировать полную сохранность этих документов в их первоначальном виде. По этой причине при изучении документов (в том числе и в архивах) обычно используют фотокопировальные папки, малогабаритные ксероксы, репродукционные устройства, фотоаппараты с удлинительными кольцами, цифровую фото- и видеотехнику, позволяющую фиксировать документы.

При сборе образцов для сравнительного исследования, например, образцов почерка, печати, штампа, места подделки документа возможно использование аппаратуры фотосъемки. Для получения отпечатков пальцев рук необходимо применение средств и методов оперативного дактилоскопирования.

При исследовании предметов и документов используются различные технические средства с целью получения информации о содержании документов, лицах, их исполнявших, способах и средствах их тиражирования, их идентификации; назначении предметов, времени, мете, технологии их изготовления; о биологических объектах (кровь, слюна, сперма, волосы).

Отождествление личности, заключаемое в установлении (оперативной идентификации) лиц, представляющих оперативный интерес, также предусматривает применение различных технических средств и методов в случаях:

- негласного опознания по признакам внешности, голосу и другим приметам;
- исследования предметов, документов, биологических объектов, фотоснимков, видео- и аудиозаписей;
- информационного поиска в оперативно-справочных, розыскных и криминалистических учетах, а также экспертно-криминалистических коллекциях и картотеках.

Следовательно, при отождествлении личности предполагаются предварительные фото-, киносъемка, видеозапись, фиксация акустической информации, проведение оперативного дактилоскопирования, а также получение пригодных для идентификации биологических объектов.

При наблюдении, в зависимости от места, времени и других обстоятельств возможно применение зрительных труб, биноклей и приборов ночного видения, перископов и других средств. При осуществлении наблюдения практически всегда возникает необходимость в фиксации действий проверяемых и разрабатываемых лиц и другой сопутствующей информации с помощью средств и методов негласного акустического и визуального контроля.

Обследование помещений, зданий, сооружений, участков местности и транспортных средств предполагает визуальное и иное изучение объектов с целью получения оперативно-розыскной информации, предусматривает применение широкого спектра средств поисковой техники, применяемых гласно или негласно, с зашифровкой цели мероприятия или без таковой. Для фиксации результатов оперативного осмотра широко используются фотосъемка и

видеозапись. Кроме того, в ходе оперативного осмотра решаются задачи, своим содержанием определяющие применение таких оперативных средств, как пометка объектов специальными химическими веществами или радиоактивными изотопами, установление химических ловушек для слеодообразования.

Уже само наименование таких ОРМ, как прослушивание телефонных переговоров и снятие информации с технических каналов связи предусматривает необходимость применения специальных технических средств.

Прослушивание телефонных переговоров обычно сопровождается звукозаписью переговоров с фиксацией номера абонента, вызываемого стоящим на контроле абонентом. В случаях применения аппаратуры автоматического опознавания номера вызывающего абонента, оперативным сотрудником, осуществляющим прослушивание либо звукозапись, фиксируется и номер вызывающего стоящего на контроле абонента.

При проведении таких ОРМ, как оперативное внедрение и оперативный эксперимент, практически невозможно обойтись без применения специальной техники, в частности, без технических средств оперативной односторонней и двусторонней связи с внедряемым сотрудником. Так, двусторонняя связь может осуществляться с помощью средств телефонной связи по заранее оговоренным паролям с абонентами телефонной сети при легендировании, с помощью портативных средств радиосвязи и т.д. Односторонняя связь может также осуществляться при помощи телефонных средств (в том числе автоответчиком), при помощи условных радиосигналов или односторонней передачи информации по каналу радиосвязи, сигналов радиомаяка (информация о нахождении внедренного лица), при помощи различных сигналов, кодов, тайников.

Говоря о последних, на наш взгляд отечественным правоохранительным структурам следует изучить и использовать в правоохранительной деятельности опыт разведки Великобритании в отношении России, получивший широкую огласку в начале 2006 года в Российских средствах массовой информации, по использованию компьютеризированных тайников и соответствующей аппаратуры прием и передачи оперативной информации.

При осуществлении контролируемой поставки нередко возникает необходимость в маркировке объектов специальными химическими веществами или радиоактивными изотопами, в применении поисковых приборов с целью выявления маркированных объектов, а также средств негласной аудио- и видеозаписи для наиболее полного документирования действий разрабатываемых лиц и других событий, имеющих отношение к проводимому ОРМ и выявляемым в его ходе правонарушениям.

Таким образом существуют следующие основные направления применения технических средств при проведении оперативно-розыскных мероприятий:

- получение оперативной информации, имеющей значение для целей борьбы с преступностью;

- документирование информации, содержащей факты подготовки или совершения преступлений, иных сведений для последующего использования в процессе уголовно-процессуального доказывания; автоматизация процессов управления субъектами проведения мероприятий;
- обеспечение информационной безопасности оперативных подразделений.

Лекция 7. ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ И ФИКСАЦИИ ИНФОРМАЦИИ

- 1. Средства обнаружения и фиксации информации.*
- 2. Понятие технического канала утечки информации. Технические средства, применяемые для дистанционного съема информации.*

1. Средства обнаружения и фиксации информации

Для получения оперативно значимой информации правоохранными органами применяются различные по назначению и конструктивным особенностям технические средства. Одни из них позволяют фиксировать получаемую информацию, то есть одновременно являются средствами документирования, другие лишь сообщают ее или способствуют ее получению. К последним относятся, например, средства визуального наблюдения: бинокли, подзорные трубы, приборы ночного видения, промышленные телевизионные установки. Получить информацию о местонахождении различных объектов, представляющих оперативный интерес, можно с помощью различных поисковых приборов. Наиболее часто в повседневной правоохранительной деятельности применяются средства фотографирования и звукозаписи. Самым эффективным средством документирования действий лиц, представляющих оперативный интерес, является видеозапись, которая дает возможность фиксировать противоправные действия в динамике с привязкой к окружающей обстановке.

В настоящее время применение разнообразных электронных средств облегчает доступ к личной жизни человека. Портативная высоконадежная аппаратура, практически вечная по сроку службы, не заметная невооруженным глазом, позволяет наблюдать за объектами с безопасного расстояния. Наибольшие возможности открывают средства дистанционного съема информации, работа которых основана на использовании так называемых побочных каналов утечки информации, достижений в сфере высоких технологий, особенно в области телекоммуникационных систем.

Таким образом, технические средства, предназначенные для обнаружения и фиксации информации, можно классифицировать на следующие группы: приборы наблюдения; поисковая техника; технические средства фиксации информации; технические средства дистанционного съема информации.

Приборы наблюдения

Известно, что более 90 % сведений об окружающем мире человек получает через органы зрения, и дополнительное использование специальных технических средств способствует расширению возможностей выявления и фиксации визуальной информации. Эти средства активно используются в практике деятельности правоохранительных органов: при организации наблюдения за встречами подозреваемых лиц, фактами передачи предметов, а также погрузки, выгрузки, выноса похищенных товаров или предметов и т. п.

По принципу действия приборы наблюдения можно разделить на четыре класса: оптико-механические; эндоскопы; электронно-оптические; телевизионные.

Оптико-механические приборы наблюдения предназначены для наблюдения за объектом на расстоянии или из-за укрытий в дневное и вечернее время суток. По функциональным возможностям их можно объединить в следующие группы:

- бинокли, монокуляры, зрительные трубы, телескопы, оптические прицелы. Главным достоинством этих приборов является увеличение масштаба изображения контролируемого объекта, что позволяет в процессе наблюдения эффективно использовать их удаленность в качестве основного фактора маскировки;

- устройства, выполненные по перископической системе, позволяющие полностью замаскировать наблюдателя в укрытии;

- инверторы дверного глазка, дополняющие стандартный глазок и дающие возможность осмотра внутреннего помещения;

- полупрозрачные зеркала, предназначенные для одностороннего наблюдения за объектом;

- объективы, представляющие собой систему оптических линз, заключенных в специальную оправу и собирающих свет, идущий от рассматриваемого через окуляр объекта;

- досмотровые комплекты зеркал, обеспечивающие возможность осмотра труднодоступных мест (межмебельных проемов, дымоходов, вентиляционных отверстий, строительных конструкций, автомобилей и т.п.).

В качестве критериев выбора того или иного вида оптико-механического прибора выступают такие тактико-технические характеристики, как фокусное расстояние, светосила объектива, угол поля зрения и другие параметры.

К данной группе приборов можно отнести, например, бинокль зеркально-линзовый с центральной фокусировкой (БЗЛ 30х60), 30-кратным увеличением, диаметром входного зрачка 60 мм и угловым полем зрения в пространстве 2

градуса, который позволяет производить наблюдение за особо удаленными объектами.

Такие устройства, как фотоснайперы (ФС-12, ФС-122, ФС-122ТК), изготовленные на базе отечественного фотообъектива «Таир-3» с фокусным расстоянием 300 мм, обеспечивают наблюдение за объектом, находящимся на расстоянии не менее 150 м.

Определенный интерес вызывает биноклярный прибор наблюдения со стабилизацией изображения (БС 16х40 «Кондор»), позволяющий вести наблюдение в условиях, осложненных тряской и вибрацией. Основу системы составляет блок призм, кинематически связанный с ротором гидростабилизирующего узла, который обеспечивает стабильное положение в пространстве визирной оси независимо от угловых колебаний самого прибора.

В процессе наблюдения за объектами используются различные типы объективов, от правильности выбора которых в немалой степени зависит успех проводимого меро-приятия. Так, длиннофокусные объективы (телеобъективы) обеспечивают качественное наблюдение объектов, находящихся на значительном удалении. К ним можно отнести такие отечественные объективы, как «Таир-3» – фокусное расстояние 300 мм, «МТО-500» (ЗМ-5АМС) – 500 мм, «МТО-1000» (МТО-11) – 1000 мм, «Гранит-11» – переменное фокусное расстояние – 80–200 мм. При их применении следует учитывать то, что увеличение кратности объектива приводит к уменьшению угла поля зрения и, следовательно, к необходимости надежной фиксации при ведении наблюдения.

Эндоскопы являются средством визуального контроля объектов окружающего пространства и труднодоступных мест (полостей и коммуникаций, внутренних поверхностей корпусов и различных блоков), где невозможен прямой обзор.

Как правило, эндоскоп представляет собой оптическую систему, состоящую из объектива, формирующего изображение, системы переноса изображения и окуляра. Рабочей частью устройства является объектив диаметром до 10 мм и система переноса изображения – стекловолоконный световод с механизмом управления объективом, заключенный в жесткую или гибкую оболочку. В некоторых устройствах предусматривается наличие блока подсветки, что расширяет их возможности.

Электронно-оптические приборы наблюдения применяются для наблюдения в помещении или на местности в ночное и вечернее время. В условиях темноты эти приборы позволяют различить силуэт человека, провести опознание лица по внешним признакам (рост, особенности походки, тело-сложение), установить номерной знак автомобиля и т. д.

Принцип действия названных приборов основан на электронном преобразовании невидимого инфракрасного излучения в видимое изображение на экране электронно-лучевой трубки. Такие преобразователи называются электронно-оптическими (ЭОП).

Инфракрасные лучи попадают в объектив электронно-оптического преобразователя и фокусируются на катоде специальной электронно-лучевой трубки. Поверхность катода покрыта особым составом из сурьмы и цезия. Под действием этих лучей в нем возникает фотоэлектронная эмиссия, в результате которой электроны вырываются с освещенных участков и под действием сильного электрического поля движутся к аноду, роль которого выполняет люминесцентный экран. Под ударами электронов экран начинает светиться, образуя видимое изображение, которое наблюдается с помощью окуляра.

Естественное инфракрасное излучение наблюдаемых объектов обычно бывает очень слабым. Для того чтобы уловить его и преобразовать в видимое изображение, требуются сложные приборы с высокой чувствительностью. Поэтому в некоторых приборах применяются источники искусственного освещения инфракрасными лучами. В качестве источника такого излучения может использоваться достаточно мощная лампа накаливания, перед которой располагается так называемый черный фильтр, задерживающий видимый спектр света и выделяющий из светового потока лампы лишь инфракрасное излучение, а также используются лазерные осветители. Лучи осветителя направляются на объект наблюдения и, отразившись от него, поступают в электронно-оптический преобразователь. Приборы с инфракрасными осветителями называются активными; приборы без осветителя, улавливающие естественное инфракрасное излучение объекта, – пассивными.

Телевизионные системы наблюдения являются важным средством в борьбе с различными видами правонарушений и находят все более широкое применение в комплексной защите объектов в качестве досмотровых и других средств.

Наибольшее применение получили замкнутые телевизионные системы, основными элементами которых являются:

- телевизионная передающая камера;
- коммутационные устройства;
- устройство отображения (телевизионный монитор);
- устройство документирования;
- линии передачи телевизионного сигнала.

Поисковая техника

Обнаружение вещественных доказательств, орудий и средств совершения преступлений, похищенных предметов и ценностей, закопанных в землю трупов и других объектов нередко имеет первостепенное значение для раскрытия преступлений и розыска преступников. Своевременное обнаружение различных запрещенных предметов особенно важно для обеспечения должного режима на обслуживаемой территории, предотвращения преступлений и иных

противоправных действий. Поиск этих объектов осуществляется с помощью приборов, которые называются поисковыми.

Поисковые приборы применяются правоохранительными органами при производстве следственных и административных действий, проведении оперативно-розыскных мероприятий (например, в целях обнаружения у проверяемых лиц ценностей, изготовленных из благородных металлов, орудий преступлений, огнестрельного и холодного оружия и других предметов, относящихся к преступной деятельности).

Поисковые приборы с учетом их целевого назначения подразделяются:

- на металлоискатели различного назначения;
- приборы для обнаружения живых существ;
- приборы для поиска взрывчатых веществ;
- приборы для поиска наркотических веществ;
- приборы для отыскания скрытых полостей и неоднородностей (пустотоискатели);
- приборы для исследования внутреннего состояния различных объектов;
- приборы для регистрации гамма-излучения;
- ультрафиолетовые осветители;
- трупоиискатели.

Металлоискатели бывают двух видов: для обнаружения черных металлов (магнитные искатели-подъемники) и любых металлов (индукционные металлоискатели).

Магнитные искатели-подъемники предназначены для обнаружения и извлечения из жидких, полужидких, сыпучих укрывающих мест (водоемов, колодцев, выгребных ям, болота, песка, снега, золы и т. п.) предметов, изготовленных из черных металлов.

Поиск в стогах сена, сугробах, кучах зерна и других подобных местах рекомендуется производить погружением подъемника в массу с последующими плавными перемещениями в разные стороны, а поиск в жидких средах – путем сканирования. После поиска подъемник извлекают на поверхность для проверки результатов. Поиск мелких предметов (обломков лезвия ножа, зубьев пилы, стружки в песке, золе) целесообразно производить, осыпая этими материалами полюсы магнита.

Для поиска изделий из любых металлов используются индукционные металлоискатели различных конструкций:

- стационарные – для массовой проверки лиц при их прохождении через пункты контроля;
- переносные – для обеспечения обысков помещений и территории;
- портативные – для личного обыска задержанных.

Указанные металлоискатели представляют собой устройства, состоящие из трех основных частей: поискового элемента, генераторно-усилительного блока и индикаторных устройств.

Стационарные индукционные металлоискатели типа «Флокс», «Гвоздика» регистрируют наличие металлических предметов у человека, проходящего через поисковый элемент, выполненный в виде дверного проема с помещенными в нем поисковыми катушками. При обнаружении металлического предмета в этих приборах включается световая и звуковая сигнализация.

Поиск переносными металлоискателями на местности рекомендуется производить по следующей методике: участок местности, где будет вестись поиск, разбивается визуально или веревочным шнуром на зоны шириной 120–150 см (при большой площади поиска местность рекомендуется разбивать на квадраты); производится сканирование поисковым элементом на расстоянии 1–5 см над поверхностью земли со скоростью 10–50 см/с; при обнаружении металлического предмета по срабатыванию индикации металлоискателя это место обозначается, и оператор останавливается; не сходя с места, он отыскивает рядом точку на поверхности, где нет металла, и в этом месте на поверхность кладется поисковый элемент прибора; помощник оператора начинает откапывать искомый предмет, насыпая грунт на поисковый элемент, что исключает выбрасывание с грунтом искомого предмета; по мере откапывания периодически обследуется место поиска для обнаружения и уточнения местоположения искомого предмета.

Портативные (ручные) металлоискатели предназначены для личного обыска и поиска металлических предметов, когда площадь поиска относительно невелика или исследуемая поверхность объекта имеет сложную конфигурацию (мебель, неметаллическая упаковка). С их помощью можно обнаружить даже очень мелкие металлические предметы.

Такие работы, как личный досмотр, осмотр посылок, упаковок и багажа, требуют от оператора освоения определенных приемов, а также предварительной подготовки. Например, для проведения личного досмотра необходимо знать, как можно использовать тело человека для укрывания каких-либо предметов. Это позволяет определить оптимальный маршрут досмотра с помощью ручного металлоискателя, который начинается, как правило, с головного убора и заканчивается обувью (как говорится, с головы до ног): прическа, головной убор, горло, грудь, живот, подмышечные впадины, внутренняя сторона рук, область половых органов, внутренняя сторона ног, ступни ног; шея, плечи, спина, поясница, кисти рук, сжатые в кулак.

Осмотр небольших неметаллических упаковок, стеклянных банок с продуктами, а также личный досмотр удобно производить, используя ручной металлоискатель. В тех случаях, когда чувствительность прибора недостаточна, можно применять переносной металлоискатель. При этом контролируемый объект, если это возможно, подносят к заранее настроенному прибору. В этом случае на руках оператора не должно быть часов, колец и других металлических предметов.

Приборы для обнаружения живых существ, укрывающихся в транспортных средствах и перевозимых в них грузах, созданы для повышения эффективности досмотровых действий на контрольно-пропускных пунктах (КПП). Они успешно заменяют служебно-розыскную собаку и широко применяются в учреждениях, исполняющих уголовные наказания.

Малогабаритный прибор «Лаванда» имеет автономное питание. Принцип его действия основан на преобразовании механических микроколебаний автомобиля, вызванных находящимся в нем нарушителем, в акустический сигнал. С его помощью можно досматривать колесные транспортные средства массой до 15 тонн. При работе прибор устанавливается на бампер автомобиля. Общее время досмотра – около двух минут. Недостатком является то, что для его применения необходим закрывающий от ветра ангар.

Применение прибора «Лаванда» будет безрезультатным, если нарушитель скрыт в грузе, хорошо поглощающем механические колебания. Это может быть резина, поролон, вата, отходы пряжи, обрезки ткани и т. п. Обычно такой груз проверяется на КПП с помощью проволочных щупов, однако он может быть спакетирован, увязан в тюки, пронизывать которые щупом невозможно.

В указанных случаях, а также при досмотре грузов в жесткой таре (ящики, контейнеры) используется другой прибор – «Гиацинт», который реагирует на продукты газообмена человека, образующиеся при дыхании («электронный нос»). Прибор работает от промышленной сети, внутренних батарей или автомобильного аккумулятора напряжением 12 В. Во время досмотра заостренная трубка газозаборного устройства вводится в естественные щели или отверстия жесткой тары либо сквозь внешнюю оболочку мягкой упаковки. При обнаружении продуктов дыхания человека в приборе загорается световой и включается звуковой сигналы тревоги.

Приборы для отыскания скрытых полостей и неоднородностей (пустотоискатели) применяются с целью обнаружения объекта сокрытия, помещенного в специальное хранилище-тайник. Принцип работы таких приборов основан на импульсном методе зондирования и регистрации сигнала, отраженного от стенок тайников, который подобно радиолокационному сигналу задерживается во времени относительно зондирующего импульса. Путем измерения времени задержки оценивается расстояние до источника сигнала, то есть определяется наличие тайника – пустоты или неоднородности плотности объекта исследования.

Приборы для исследования внутреннего состояния различных объектов. К данной группе приборов относится специальная рентгеновская аппаратура, с помощью которой можно исследовать объекты и предметы как в стационарных, так и в полевых условиях.

Ультрафиолетовые осветители позволяют обнаружить метки, сделанные специальными химическими веществами, и объекты органического происхождения, такие как слюна, кровь, сперма.

Трупоиискатели. Принцип действия трупоиискателей первой группы основан на проведении реакции выявления содержания сероводорода в контролируемом пространстве, а второй группы – изменении проводимости почвы, возникающем при разложении трупа.

Широкого применения в деятельности правоохранительных органов трупоиискатели не нашли, так как нередко происходило ложное срабатывание на гниlostное разложение объектов органического происхождения. В настоящее время с вооружения сняты. Однако ведутся опытные разработки подобных изделий на современной технической и технологической основе, использующих в комплексе принципы радиолокационного зондирования и газоанализа.

Технические средства фиксации информации

Опыт показывает, что без широкого применения средств фиксации информации часто невозможно или крайне затруднительно документировать преступные действия. Это связано с условиями высокой скрытности совершаемых преступлений и профессионального противодействия преступных структур. В то же время правильное и своевременное их использование позволяет выявлять и раскрывать самые сложные и запутанные преступления.

Разработанная на основе новейших технологий для правоохранительных органов техника фиксации информации отличается такими специфическими тактико-техническими возможностями, как повышенная надежность, простота обслуживания, малогабаритность, расширенный температурный диапазон эксплуатации.

К техническим средствам фиксации информации относятся средства фото-, видео- и аудиозаписи. Они позволяют зафиксировать, длительно хранить и использовать в процессе дальнейшей оперативно-розыскной деятельности, предварительного и судебного следствия результаты визуальных наблюдений и аудиозаписей за лицами и объектами, представляющими интерес для правоохранительных структур.

Анализ борьбы с преступностью показывает, что средства фиксации информации могут эффективно использоваться не только в следственной деятельности, но и для получения информации при проведении оперативно-розыскной деятельности, которая связана с документированием действий, свидетельствующих о подготовке и совершении преступлений, фиксацией фактов встреч лиц, а также документов, результатов осмотра мест происшествий, внешнего вида орудий или следов преступной деятельности и т. д.

В настоящее время применение техники фиксации информации приобрело важное значение. Это во многом связано с проблемами обеспечения свидетельской базы при документировании преступных действий, к которым можно отнести запугивание свидетелей и потерпевших, низкую активность населения в оказании помощи правоохранительным органам и т. д.

Таким образом, применение техники фиксации информации обеспечивает:

- фиксацию лиц и их действий;
- фиксацию материальных носителей в случае, когда документы или предметы, представляющие интерес, могут быть подделаны, уничтожены или скрыты;
- фиксацию результатов осмотра мест происшествий и других следственных действий, а также внешнего вида орудий и следов преступной деятельности;
- последующее установление активных участников массовых беспорядков и групповых хулиганств.

Согласно принятой классификации можно выделить следующие технические средства фиксации информации: фотосъемки; репродукционной и фотокопировальной съемки; аудиозаписи; видеозаписи.

Средства фотосъемки. К ним относятся фотокамеры, наборы сменной оптики, светофильтры, бленды, экспонометры и иные приборы, принадлежности и устройства, необходимые для осуществления съемочного процесса.

В практике деятельности правоохранительных органов используется различная фотоаппаратура, которую условно можно разделить на две основные группы: общего и специального назначения. К первой группе относится аппаратура для профессиональной и любительской съемки, а ко второй – специально разработанная техника. Из технических средств первой группы широко применяются различные фотокамеры, объективы и другие принадлежности.

Фотокамеры общего назначения принято классифицировать по формату кадра, конструктивным особенностям, типу затвора, степени автоматизации различных функций и т. д.

В последние годы широко используются цветные цифровые фотокамеры. Полученное изображение преобразуется в числовую форму и передается в запоминающее устройство фотокамеры.

Для проведения фотосъемки на значительном расстоянии приближение объекта выполняется в помощью телеобъективов, что обеспечивает качественную съемку даже сильно удаленных объектов.

В отдельную группу можно выделить объективы с малым входным отверстием. Объектив типа Pin-hole, что дословно переводится как «игольчатая дырочка», имеет диаметр от 0,8 до 4 мм и применяется, например, для скрытой фиксации информации и в оптических эндоскопах.

Для получения фотокопий таких бумажных носителей, как товарно-транспортные накладные, оттиски печатей, штампов, применяются малогабаритные репродукционные устройства.

В настоящее время для репродуцирования фотографий, документов и их фрагментов используются фотоаппараты для макросъемки и устройства ксерокопирования.

Средства аудиозаписи. Технические средства фиксации информации позволяют осуществлять аудиозапись речевой информации в различных условиях: на открытой местности, в салонах транспортных средств, помещениях и т. д.

В качестве технических средств аудиозаписи используются малогабаритные диктофоны и магнитофоны. С помощью звукозаписывающей аппаратуры могут быть решены следующие задачи:

- получение аудиоинформации о противоправной деятельности лиц, обоснованно подозреваемых в преступных действиях;
- документирование преступных деяний путем объективной регистрации речевых сообщений, иных звуков для последующего использования в качестве доказательств;
- фиксация в режиме реального времени и накопление речевых сообщений большого объема за длительный период для последующего анализа.

Средства аудиозаписи, применяемые в правоохранительной деятельности, в зависимости от основных тактико-технических возможностей можно подразделить на три группы: стационарные; переносные; малогабаритные.

К первой группе относится аппаратура, установленная в дежурных частях для записи автоматически в режиме реального времени речевой информации, поступающей по радио- и телефонным каналам связи. К этой же группе можно отнести и многофункциональные системы регистрации речевой информации, например на базе ПК.

Ко второй группе относятся магнитофоны и диктофоны, используемые для фиксации информации при проведении оперативных и следственных действий.

Третью группу составляют малогабаритные аппараты магнитной записи, применяемые при проведении оперативно-розыскных мероприятий.

Средства звукозаписи также могут быть двух видов: общего назначения (бытовые) и специально разработанные (или адаптированные) для деятельности правоохранительных органов.

Таким образом, состав техники магнитной записи, используемой в правоохранительных органах, весьма разнообразен: от бытовых магнитофонов и диктофонов до специально разработанных устройств с современной технологией аудиозаписи.

Средства видеозаписи. В деятельности правоохранительных органов для проведения видеосъемки применяются, как правило, зарубежные бытовые и профессиональные портативные видеокамеры, а также специальная видеоаппаратура, предназначенная для негласного получения информации.

К аппаратуре видеозаписи относят видеокамеры, видеоманитофоны, мониторы и различные аксессуары (блок питания, соединительные шнуры, адаптер и др.). Так же как и фототехника, видеокамеры могут быть снабжены объективами с переменным или постоянным фокусным расстоянием. В качестве

монитора может быть использован любой телевизионный приемник, дисплей персонального компьютера.

Осуществляя видеосъемку, необходимо соблюдать следующие правила: желательно снимать отдельными фрагментами и на разных съемочных планах, обеспечивающих необходимую акцентированность и композиционную выразительность изображения. Съемочные планы подразделяются на общие, средние и крупные. Тот или иной съемочный план достигается путем смены фокусного расстояния объектива видеокамеры или съемкой с различных по удаленности от снимаемого объекта точек. Съемку конкретных эпизодов проводят непрерывно.

Осуществляя фрагментарную съемку, следует иметь в виду, что два смежных фрагмента, если они друг от друга ничем не отделены, воспринимаются зрителем как единое целое. Поэтому нужно отделять один фрагмент от другого с помощью затемнения. Это можно сделать быстро, например, закрыв рукой на 2-3 с объектив видеокамеры.

Начинают съемку обычно с общего плана, чтобы при просмотре было понятно, где происходит действие, в какой местности, в какое время года, то есть общие планы должны быть информационного характера. Особенно важно, чтобы они содержали указание на то, где происходит снимаемое действие. Для большей конкретности информации общие планы могут чередоваться с крупными, на которых фиксируются детали обзорного характера (например, таблички с названиями улиц, вывески магазинов). Конкретные действия разрабатываемых лиц снимаются средним планом.

Для более четкого восприятия мелких деталей (лица, рук, предметов, денег, документов, этикеток и надписей на упаковке товаров) их снимают крупным планом.

Возможность видеокамеры записывать звук позволяет не только зафиксировать разговор разрабатываемых лиц, но и комментировать их действия во время съемки.

3. Понятие технического канала утечки информации. Технические средства, применяемые для дистанционного съема информации

Несанкционированный доступ к конфиденциальным сведениям может быть организован «извне», путем проведения разведывательных мероприятий, реализующих съем информации с технических каналов утечки информации.

Под техническим каналом утечки информации принято понимать систему, в состав которой входят:

- 1) объект разведки;

2) техническое средство, используемое для несанкционированного получения нужных сведений;

3) физическая среда, в которой распространяется информационный сигнал.

Объектом разведки могут быть помещение, группа помещений или здание с хранящимися материалами ограниченного пользования, технические каналы связи, используемые для передачи сведений, а также участки местности и транспортные средства.

Арсенал технических средств, с помощью которых добывается информация, весьма обширен: это средства фото- и видеодокументирования, специальные микрофоны, стетоскопы и лазерные акустические системы, системы радиоперехвата, средства съема информации с проводных линий связи и др.

Физическая среда, в которой распространяются информационные сигналы, имеет различную природу. Это могут быть строительные конструкции зданий и сооружений, токопроводящие линии, среда распространения акустических сигналов, электромагнитные поля. Средой распространения информации являются также технические средства обработки информации, находящиеся в помещении, – вычислительная техника, автоматические телефонные станции, системы звукозаписи. Кроме них, имеются и другие технические средства и коммуникации. Так, все помещения, как правило, электрифицированы и телефонизированы, в них должны быть проложены проводные линии электропитания, установлены приборы освещения, различная электробытовая техника, система охранно-пожарной сигнализации. Непосредственно не используемые в процессе обработки информации технические системы и средства принято называть вспомогательными.

Выделяют следующие группы основных технических каналов утечки информации: электромагнитные; электрические; оптические; акустические.

Электромагнитные каналы утечки информации. К ним относят каналы утечки информации, возникающие за счет побочных электромагнитных излучений технических средств обработки информации.

Вся работающая электронная аппаратура и электронные системы, на какой бы технической базе они ни формировались – от телефонного аппарата до современных компьютерных систем, а также проводные коммуникации создают электромагнитные поля, называемые побочными электромагнитными излучениями. Они способны создавать электромагнитные наводки в расположенных рядом слаботочных, силовых и осветительных сетях, линиях и аппаратуре охранно-пожарной сигнализации, проводных линиях связи, различных приемниках электромагнитных излучений.

В результате таких процессов возникают каналы утечки информационных сигналов, так как электрическое поле, создаваемое работающей аппаратурой, является носителем обрабатываемой или передаваемой информации. Специальные широкополосные приемники позволяют «считывать»

электромагнитные излучения, а затем восстанавливать и отображать содержащуюся в них информационную составляющую.

Электрические каналы утечки информации могут возникать за счет:

- наводок электромагнитных излучений технических средств обработки информации на коммутационные линии вспомогательных технических систем и средств;

- утечек информационных сигналов в цепях питания технических средств обработки информации;

- утечек информационных сигналов в цепях заземления технических средств обработки информации:

Например, побочные электромагнитные поля работающих компьютеров производят наводки на близко расположенные коммутационные линии вспомогательных средств и систем, к которым можно отнести: охранно-пожарную сигнализацию, телефонные провода, сети электропитания, металлические трубопроводы, цепи заземления. В этом случае возможен съем информации путем подключения специальной аппаратуры к коммуникационным линиям за пределами контролируемой территории.

Оптические каналы утечки информации. Несанкционированное получение оптической информации осуществляется путем наблюдения за объектом, при необходимости может вестись фото- или видеосъемка. Различных видов технических средств, используемых в целях получения информации, достаточно много – это бинокли, приборы ночного видения, фото- и видеотехника и др.

Акустические каналы утечки информации. Наиболее распространенным способом несанкционированного доступа к информации является перехват акустической (речевой) информации.

Каналы утечки акустической информации принято классифицировать следующим образом: электроакустический; виброакустический; акустический; оптико-электронный; проводной; электромагнитный.

Электроакустический канал утечки информации. Ряд элементов вспомогательных технических систем и средств (прежде всего громкоговорители трансляционной сети, звонки телефонных аппаратов и др.) меняют свои электрические параметры (емкость, индуктивность, сопротивление) под действием акустического сигнала. Изменение параметров вызывает модуляцию информационным сигналом токов, протекающих в элементах вспомогательных технических средств и систем. Такие электрические преобразования получили название «микрофонный эффект». Рассмотрим его действие на примере телефонного аппарата, поскольку утечки речевой информации по открытым телефонным каналам представляют собой серьезную угрозу.

С точки зрения безопасности телефонный аппарат имеет существенный недостаток, поскольку его основные узлы (микрофон, наушник, звонковая цепь) могут выполнять функции приемника и передатчика сигналов при

несанкционированном прослушивании помещения, в котором он установлен. Звонковая цепь телефонного аппарата при положенной на рычаг трубке создает микрофонный эффект. Подвижные части звонка вибрируют под действием речевых сигналов (разговор в помещении), что приводит к появлению в нем электрического тока малой амплитуды. Это, в свою очередь, позволяет провести соответствующую обработку возникающего в цепи сигнала и выделить звуковую составляющую за пределами контролируемого помещения.

Другим способом снятия информации с телефона является высокочастотное навязывание. Суть этого метода состоит в подключении к одному из проводов телефонной линии высокочастотного генератора, работающего в диапазоне 50–300 кГц. Правильный подбор частоты генератора и частоты резонанса телефонного аппарата позволяет при положенной трубке добиться модуляции высокочастотных колебаний микрофоном, который улавливает звуковые сигналы в прослушиваемом помещении. Существует и ряд других приемов превращения телефонного аппарата в технический канал утечки информации.

Виброакустический канал утечки информации реализуется путем использования электронных стетоскопов. При этом происходит снятие результатов воздействия акустических речевых сигналов на строительные конструкции и сооружения (панели перегородок стен, пол, потолок, воздуховоды, вентиляционные шахты, трубы и батареи отопления, оконные стекла и т.д.). Под воздействием акустических волн строительные конструкции подвергаются микродеформации, в результате которой возникают упругие механические колебания, хорошо передающиеся в твердых однородных средах. Эти колебания воздействуют на чувствительный элемент электронного стетоскопа (вибродатчик) и преобразуются в электрический сигнал, который затем усиливается и может быть передан по проводным, оптическим или радиоканалам связи. Этот метод достаточно эффективен, так как не требует проникновения в контролируемые помещения. Такой стетоскоп легко устанавливается за пределами контролируемой зоны (на элементах строительных конструкций, трубах водоснабжения и отопления).

Оптико-электронный канал утечки информации. Акустический контроль удаленных помещений, имеющих окна, может быть осуществлен с использованием оптико-электронных, или, как их нередко называют, лазерных, систем (лазерных микрофонов).

Современные лазерные системы позволяют осуществлять прослушивание разговоров, ведущихся в помещении, на расстоянии от 100 м до 1 км. Для отражения лазерного луча могут быть использованы также элементы мебели и интерьера – стеклянные поверхности и зеркала внутри помещения.

Лазерные системы состоят из источника когерентного излучения (передатчика) и приемника отраженного луча. Передатчик представляет собой оптико-электронное устройство, формирующее луч и направляющее его в нужную точку отражающей поверхности, например на оконное стекло

помещения, в котором ведутся переговоры. Отраженное излучение модулируется речевым (акустическим) сигналом, который возникает в помещении при ведении переговоров, улавливается приемником, демодулируется с последующим шумоподавлением и усилением.

Отметим, что серьезным недостатком таких систем является их зависимость от гидрометеорологических условий – дождь, снег, туман, порывистый ветер в значительной степени затрудняют съем информации или делают его невозможным.

Акустический канал утечки информации. Самым простым способом перехвата речевой информации, не требующим использования специальной техники, является подслушивание ведущихся разговоров. Неплотно прикрытая дверь в кабинет должностного лица, обсуждение сведений ограниченного распространения в курительной комнате или за пределами служебных помещений, конфиденциальное совещание, проводимое в помещении с открытыми окнами, – вот те простые, но вместе с тем вполне реальные каналы утечки информации.

Если при этом лицо, проявляющее интерес к чужим тайнам, использует такие технические средства, как направленный микрофон, скрытый в стенке портфеля или внутри зонта, и портативный диктофон, то это с высокой степенью вероятности позволит не пропустить ни одного слова и зафиксировать контролируруемую беседу.

Проводной канал утечки акустической (речевой) информации. В зданиях и сооружениях причиной возникновения акустических каналов являются воздуховоды, вентиляционные шахты, щели и пустоты в некачественных строительных материалах, а также специально сделанные отверстия в потолках, стенах, полах.

Для снятия акустической информации могут быть использованы проводные микрофоны, которые через линии связи подключаются к звукоусилительной и звукозаписывающей аппаратуре.

В качестве канала передачи перехваченной информации используются телефонные линии и линии вспомогательных технических средств и систем, силовая и осветительная сеть, оптический и инфракрасный каналы, при этом информация передается за пределы контролируемой зоны в закодированном виде либо без кодировки.

Электромагнитный канал утечки информации. Наряду с направленными микрофонами, диктофонами и лазерными системами для несанкционированного съема речевой информации широко используются скрытно устанавливаемые акустические закладные устройства, или радиомикрофоны.

Такие устройства изготавливаются как камуфлированными, так и без камуфляжа. Они скрытно устанавливаются во вторичных технических средствах и системах, а также технических средствах обработки информации. Местом установки могут быть: телефонный аппарат, электрические розетки,

выключатели и т. п. Нередко осуществляется их маскировка в настольных предметах (пепельницы, письменные приборы, вазы для цветов), предметах мебели и интерьера, элементах конструкций зданий и др.

В качестве источника питания закладного устройства может использоваться электрический ток силовой, осветительной или телефонной сети за счет гальванического подключения или использования специальных сетевых блоков питания, а также детектора СВЧ-энергии. Закладное устройство может иметь независимый источник электропитания – химический или радиоизотопный, солнечную батарею и др.

Существуют радиомикрофоны непрерывного действия (постоянно включенные), дистанционно управляемые (включаются по команде оператора), а также с акустопуском (система VOX) – при появлении речевого сигнала в контролируемом помещении происходит самовключение устройства.

Лекция 8. ИСПОЛЬЗОВАНИЕ В ПРЕДОТВРАЩЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ ПОЛИГРАФНЫХ УСТРОЙСТВ

1. История создания и физиологические основы проведения опроса с применением полиграфных устройств.

2. Принципы построения различных типов полиграфных устройств.

3. Методические особенности использования полиграфных устройств при опросе.

1. История создания и физиологические основы проведения опроса с применением полиграфных устройств

В настоящее время в работе правоохранительных органов все более широкое применение находят нетрадиционные методы раскрытия преступлений, основанные на современных достижениях науки и техники. Одним из примеров применения таких методов может служить использование современных достижений науки в изучении психологии и высшей нервной деятельности человека при проведении полиграфных исследований.

Полиграф (детектор лжи, лай-детектор, полискрайбер, плетизмограф, сфигмограф) представляет собой совокупность технических устройств, контролирующих ряд физиологических параметров человека (частоту дыхания, пульс, давление крови, электроподвижность кожного покрова, его поверхностные термальные зоны) и специальные методики установления стрессового реагирования опрашиваемого на задаваемые вопросы по изменению параметров в целях определения наличия лжи или неискренности в ответах.

Каждая из психофизиологических характеристик человека имеет свои особенности, хотя управляется единым органом – вегетативной нервной

системой. В основе принципа действия полиграфных устройств лежит контроль психофизиологических реакций организма человека на внешние раздражители в виде специальных тестов. Если в процессе тестирования регистрировать динамику изменения психофизиологических реакций с помощью полиграфа и логически сопоставлять их с содержанием вопросов теста, то с определенной степенью точности можно судить о колебаниях уровня эмоциональной напряженности и, следовательно, повышенного реагирования на те или иные конкретные вопросы.

Цель использования человеком лжи – с помощью вербальных и невербальных средств коммуникации дезинформировать партнера, ввести его в заблуждение относительно истинного положения дел в обсуждаемой области.

Определение лжи и неискренности в ответах основывается на том факте, что человек, произносящий заведомую ложь, испытывает в этот момент некоторый психологический стресс, вызывающий, в свою очередь, физиологические изменения в его организме.

Такие факторы, как измененный размер зрачка и пересохший рот, использовались на протяжении веков для того, чтобы определить, лжет человек или говорит правду.

Один из древних китайских способов установления преступника среди подозреваемых состоял в том, что всем им предлагалось наполнить рот измельченным рисом и отвечать на задаваемые вопросы судьи мимикой и жестами. Если после завершения процедуры допроса у одного из них рис оставался сухим, этот человек мог быть признан виновным в расследуемом преступлении. Объяснение этому достаточно простое – страх перед разоблачением вызывает стресс и, как следствие, физиологическую реакцию организма, ограничивающую работу слюноотделительных желез (сухость во рту). В этих же целях в Англии в средние века подозреваемым во время допроса предлагали жевать старый сухой сыр. Кроме того, нередко давалось психологическое объяснение изменения частоты пульса. Аналогичным образом в некоторых африканских странах до сих пор используют эффект стрессовой активности движений конечностей тела (тремор) лгущего человека, испытывающего страх перед наказанием в случае разоблачения, применяя оригинальный индикатор. Так, допрашиваемым подозреваемым предлагают держать в руках очень хрупкие яйца одного из видов птиц. Если скорлупа лопнет, то державший их человек будет рассматриваться в качестве лица, причастного к расследуемому преступлению.

Применение подобных способов – попытка интуитивного использования внешних двигательных и физиологических реакций в качестве индикатора реагирования на эмоциональные раздражители. При всей своей простоте, а порой примитивности, они основаны на реальном механизме психофизиологических реакций в современном представлении.

Действительно, эмоциональное напряжение лгущего человека может быть выявлено различными путями: начиная с логического анализа поведенческих реакций и заканчивая визуальной и слуховой фиксацией внешних проявлений изменения физиологических параметров при сильном эмоциональном напряжении (покраснение лица, изменение частоты, темпа, амплитуды и иных слышимых параметров голоса, дрожание конечностей, расширение зрачков и т. п.).

История создания полиграфа относится к концу XIX в. Еще в 1875 г. итальянский физиолог Моссо демонстрировал опыты по изменению давления крови и частоты пульса в зависимости от попыток скрыть правду при ответах на во-просы. В пользу применения приборов для «диагностики лжи» выступали в 1908 г. психиатр Мюстерберг (США), в 1914 г. – Бенуси (Германия). Активная разработка приборов типа «полиграф» и их применение в борьбе с преступностью в США стали осуществляться с начала 20-х годов. В конце Второй мировой войны широкое использование этих средств американской контрразведкой в лагерях военнопленных, дислоцированных на территории Германии, придало значительный импульс технико-психологическому совершенствованию полиграфных устройств. В послевоенные годы именно спецслужбы разведки и контрразведки, прежде всего США, стали основными заказчиками таких средств. Значительные финансовые ассигнования спецслужб и обширные научно-технические связи этих органов в академических и других исследовательских учреждениях позволили использовать самые современные достижения науки и техники для совершенствования полиграфа. Попытки применять его в сочетании с наркотиками, которые депрессирующим образом действуют на нервную систему и растормаживают сдерживающие центры человека, привели к ошутимым результатам.

Одновременно стали проводиться исследования в области психологической тренировки разведчиков в целях противодействия применению полиграфа и наркотиков. В частности, американские специалисты считают, что тренированный человек, имеющий необходимые потенциальные психологические качества, способен успешно скрывать правду в таких ситуациях.

Исследования и практику разведывательных служб США в области применения полиграфа при допросе широко заимствовала полиция зарубежных стран для использования в оперативной работе и даже уголовном процессе. В целях технического обеспечения такого использования применяют самые современные достижения науки и техники: тепловидение, бесконтактные датчики измерения кровяного давления и частоты пульса, электронно-вычислительную технику. Существенное развитие получила и методика опроса подозреваемого с помощью полиграфа, которая основана на достижениях психологии и исследований высшей нервной деятельности человека.

В 70–80-х годах на страницах юридической и специальной литературы развернулась острая дискуссия о возможностях использования полиграфа в уголовном процессе и оперативно-розыскной деятельности.

Полиграфы нашли широкое распространение в уголовном процессе США, Японии, Великобритании, Польши, Венгрии, Чехии, Словакии и других стран, активно используются в ходе предварительного расследования по тяжким преступлениям.

В практике зарубежных правоохранительных органов полиграфные исследования осуществляются по двум основным направлениям: в оперативной работе и уголовном процессе. Последнее подвергалось острой критике со стороны большинства ученых-юристов, специалистов в области уголовного процесса и судопроизводства.

Неприятие полиграфа в советском уголовном процессе объяснялось прежде всего тем, что в основу использования такого средства положено якобы психическое принуждение, ведущее к нарушению прав человека, а также научной необоснованностью получаемых с его помощью результатов.

Основные аргументы против применения полиграфных исследований формулировались следующим образом:

- нарушение прав человека и конституционных гарантий, противоречие законодательным нормам уголовного процесса и судопроизводства;
- отсутствие глубокой научной проработки психологии и физиологии высшей нервной деятельности с позиции методики и техники полиграфа;
- недопустимость использования результатов полиграфных исследований в уголовном процессе как средства, не дающего полной гарантии определения правды и лжи;
- несовершенство технических средств и методик применения полиграфа, потенциальная возможность различной трактовки показаний приборов, субъективизм в их оценке;
- возможная некомпетентность специалистов, использующих полиграф.

Однако ряд ученых стоят на иных позициях, высказывая мнение о возможности применения таких устройств в процессе предварительного следствия и оперативно-розыскной деятельности. Они аргументируют свои доводы положительными результатами, достигнутыми за рубежом, и доказанной эмпирическим путем взаимосвязью (в большинстве случаев) физиологических характеристик с изменением в эмоциональном состоянии, вызванном боязнью разоблачения в ходе опроса на причастность к противоправному деянию. При этом выдвигается несколько контраргументов.

Во-первых, применение полиграфов не может рассматриваться как нарушение прав человека и конституционных гарантий неприкосновенности личности, так как отсутствует элемент принуждения и в основу принятия решения о проведении полиграфных испытаний положен принцип добровольности. Вопрос состоит в том, как создать механизм контроля, чтобы

исключить возможные злоупотребления, например, оказание психологического давления для получения согласия на проведение полиграфных испытаний. Реальный путь решения этой проблемы – подробное ведомственное регулирование применения полиграфов с документальным закреплением согласия испытуемого.

Во-вторых, недостаточность научной проработки психологии и физиологии высшей нервной деятельности с позиций методики и техники применения полиграфа вполне может быть компенсирована отечественными исследованиями или заимствованными в установленном порядке результатами зарубежных исследований в этой области.

В-третьих, ограничение сферы применения полиграфов только решением задач оперативно-розыскного характера исключает прямое использование полученных результатов в процессе доказывания. Применение этих сведений в качестве наводящей (поисковой) информации не требует их абсолютной надежности.

В-четвертых, техника и методика проведения полиграфных испытаний в современных условиях имеют довольно высокий уровень надежности, вполне приемлемый для решения оперативно-розыскных задач.

В-пятых, возможная некомпетентность специалистов, использующих полиграф, может оцениваться по аналогии с некомпетентностью эксперта или специалиста в уголовном процессе и требует лишь принятия соответствующих мер по их обучению и контролю.

Современные достижения в области техники, судебной психиатрии и методике использования полиграфа, других психологических наук, создание принципиально новых модификаций датчиков физиологического состояния человека бесконтактного типа побудили многих ученых к пере-осмыслению оценки применения таких устройств в деятельности правоохранительных органов.

2. Принципы построения различных типов полиграфных устройств

К полиграфам относятся приборы, использующиеся для фиксации психологических параметров (реакций) человека посредством датчиков. Получение информации может осуществляться с помощью как контактных, так и бесконтактных датчиков (речевые и термальные измерители стресса).

В настоящее время известно три основных типа полиграфных устройств: обычный полиграф; сигнализатор психологического стресса; тепловизор.

Действие *обычного полиграфа* основано на химических изменениях в организме человека, испытывающего психологический стресс. При этом повышается содержание адреналина в крови, увеличивается потребность организма в кислороде, что, в свою очередь, вызывает увеличение частоты

пульса, повышение кровяного давления, частоты и глубины дыхания. Когда источник стресса исчезает, организм вырабатывает норадреналин, нейтрализующий действие избыточного адреналина.

Обычный полиграф представляет собой устройство, состоящее из контактных датчиков, которые устанавливаются на теле человека (голове, руках, в области сердца, легких и т. д.), и приборов, отображающих в наглядной форме информацию, получаемую с этих датчиков. Для отображения данных полиграфных исследований используется не менее двух датчиков-самописцев: кардиографический и пневмографический.

Кардиографический датчик получает информацию с помощью надувной манжеты, надеваемой на руку испытуемого, которая соединяется с устройством отображения информации – пишущим прибором, регистрирующим изменения кровяного артериального давления и частоты пульса.

Пневмографический датчик представляет собой трубку (две трубки), которой (которыми) охватывают грудь испытуемого и строят один или два пневмографика.

В некоторых моделях обычного полиграфа применяется еще один показатель – относительная электрическая проводимость кожи. В этом случае два электрода закрепляют на двух пальцах одной руки и подключают к омметру. Исходный уровень устанавливается исследователем. Отклонения от исходного уровня указывают на увеличение или уменьшение проводимости кожи. Однако этот показатель не отражает реальных стрессовых ситуаций и поэтому отвергается многими исследователями.

К недостаткам обычного полиграфа можно отнести то, что исследование с его применением требует от испытуемого полной неподвижности, так как любое движение способно вызвать изменение пульса, давления и дыхания (ноги закреплены на полу, руки пристегнуты к подлокотникам кресла, допускаются только односложные ответы «да» и «нет», на руке – надувная манжета, грудь охватывает трубка). Такая процедура сама по себе способна вызвать стресс и затрудняет обнаружение изменений, вызванных лживыми ответами. К тому же реакция адреналиновых желез может быть не связана с задаваемыми вопросами.

Достаточно известны полиграфы фирмы «Lafayette» (США), которая выпускает портативные и стационарные комплексы полиграфов. Эти устройства используются для измерения психофизического состояния человека, в том числе при проведении расследований полицией, службой безопасности и частными детективами. Четырех-пятиканальные полиграфы позволяют фиксировать на обычной бумаге чернилами или на термобумаге показания кожно-гальванической реакции человека, дыхания и кровообращения, частоту сердечных сокращений. Они комплектуются специальными креслами с различными датчиками, в том числе датчиком движений. Также возможно подключение к компьютеру.

Научно-исследовательский институт специальной техники МВД России на базе ПК разработал аппаратурно-программный комплекс экспресс-диагностики психофизического состояния человека «Корректор», который позволяет измерять кожно-гальваническую реакцию, частоту сердечных сокращений и дыхания, электрокардиограмму человека. Результаты исследования представляются в табличном и графическом виде. Прибор выпускается в стационарном и портативном вариантах. Габариты основного блока – 265x165x50 мм.

В настоящее время на вооружение органов внутренних дел принят *сигнализатор психологического стресса (PSE)*, разработанный в 1970 г., запатентованный в США, Великобритании, Канаде и Японии, широко применяющийся в оперативной работе. PSE отражает неврологические изменения. Принцип его действия основан на том, что в человеческом организме существует явление, называемое психологической дрожью, или мускульной микродрожью. Эта дрожь может проявляться как кратковременные колебания или волнообразные движения работающих мышц. Величина колебаний наибольшая, когда человек находится в беспокойном состоянии, и убывает пропорционально уменьшению уровня стресса.

Мембраны, образующие голосовые связки, управляются тремя группами мышц, придающими им определенную форму. Воздух, проходя через них, создает звук, высота которого частично зависит от напряжения мышц. Эффект мышечной микродрожжи способен в небольших пределах влиять на частоту звука, изменяя ее пропорционально величине дрожи. Отклонения настолько малы, что не улавливаются человеческим ухом. Тем не менее этот эффект проявляется как в частотной модуляции голоса, так и в изменении его тембра. Мышечные вибрации происходят в диапазоне от 5 до 15 Гц, и соответственно в этих же пределах изменяется звучание.

В отличие от классического полиграфа названные устройства позволяют регистрировать и измерять, а также фиксировать в наглядной форме основные компоненты человеческого голоса, то есть в нормальных условиях в голосе человека присутствует частотная характеристика в пределах 5–15 Гц. В условиях эмоционального стресса эти колебания, независимо от воли человека, подавляются.

Принцип определения такого стресса основан на анализе частотных характеристик с помощью специальной аппаратуры. Когда человек говорит в состоянии стресса, вызывая снижение модуляции, полиграф реагирует на частотную демодуляцию голоса (основную и тембровую). Исчезновение указанного компонента в голосе человека может косвенно свидетельствовать о его волнении, которое в сопоставлении с содержанием беседы показывает причины этих изменений, в том числе повышенное эмоциональное реагирование на конкретную информацию, а следовательно, неискренность в показаниях. При этом данные устройства служат не для установления правды и

лжи, а для выявления уровня стресса. Конечные рекомендации по оценке полученных результатов относятся к сфере психологии и оперативно-розыскной деятельности.

Таким образом, сигнализатор психологического стресса, помимо определения низкочастотного микромышечного дрожания, позволяет измерять и анализировать в комплексе такие параметры речи человека, как единичное респираторное произнесение, быстроту закрывания голосовой щели, продолжительность произнесения, присутствие или отсутствие дополнительной вибрации в голосе как результат изменения кровяного давления, изменение высоты (тембра) звука.

Комплексный анализ указанных параметров дает возможность определять общее нервное напряжение и величину эмоционального стресса.

Обработку сигнала осуществляет компьютерная техника, которая позволяет избавиться от побочной информации и обеспечивает более простую форму представления результата.

К преимуществам сигнализатора психологического стресса, отличающим его от обычного полиграфа, необходимо отнести следующие:

1. Поскольку в качестве источника определения стресса используется голос, нет нужды прикреплять к телу испытуемого какие-либо приборы, что снижает общий уровень стресса.

2. Благодаря тому что используется невралгический симптом стресса, а не медленно протекающая химическая реакция, устраняются задержки в проведении исследования и становится возможным задавать вопросы в нормальном темпе.

3. Испытуемый может отвечать многосложно, что устраняет неестественность. Двусмысленные ответы обрабатываются с такой же достоверностью.

4. Так как источником определения стресса является голос, исследоваться могут запись голоса, сигнала радио, телевидения, телефона и даже сохранившиеся записи голосов давно умерших людей.

5. PSE проводит точное измерение, тогда как обычный полиграф дает лишь приблизительную оценку. Определение уровня стресса не требует сравнения с другими ответами, то есть он может быть совершенно самостоятельно оценен при использовании любой фразы или звука.

В оперативной работе применяются такие приборы, как сигнализатор психологического стресса «PSE-101» и голосовой анализатор стресса «MARK II».

Сигнализатор психологического стресса «PSE-101», изготовленный фирмой «Dektor», одобрен более чем 3000 пользователей и несколькими десятками исследований на достоверность. Метод определения голосовых модуляций, вызываемых стрессом, на котором основано действие этого прибора, защищен американским патентом. Прибор размещен в атташе-кейсе.

Голосовой анализатор стресса «MARK II» был запатентован Ф. Фуллером спустя два года после появления «PSE-101». Прибор снабжен цифровым дисплеем и печатающим устройством, что делает возможным последующий анализ результатов, размещается в атташе-кейсе. В комплект входят: кассетный магнитофон, ролики для графопостроителя, выносной микрофон, телефонный адаптер и обучающая кассета. Габариты прибора – 33х14х43 см, вес – 26 кг, питание от сети – 120–240 В (50/60 Гц).

Кроме сигнализатора психологического стресса, созданы и иные виды бесконтактного полиграфа. Наибольший интерес вызывают устройства, основу которых составляют так называемые *тепловизоры*. Принцип их действия основан на том, что кожный покров лица человека на разных участках имеет различную температуру. Получаемое с помощью тепловизора изображение лица человека позволяет посредством анализа цветовой гаммы контролировать динамику изменения температуры термальных зон лица человека с точностью до $0,01^{\circ}\text{C}$.

Опытным путем доказана зависимость изменения температуры термальных зон от эмоционального состояния человека: при волнении она повышается, особенно на участке лобной части и щек. Обычным визуальным наблюдением выявить такие изменения довольно трудно. Лишь при сильном возбуждении повышение температуры и расширение кровеносных сосудов вызывают изменение цвета лица, причем оно очень зависит от состояния кровеносных сосудов. Использование тепловизора позволяет с большой точностью судить об изменениях температуры по смене цветовых гамм. Конкретные показатели определяются по специальной таблице цветов.

Применение тепловизора в качестве бесконтактного полиграфа заключается в следующем: передающая камера тепловизора направляется на опрашиваемого и передает на экран цветного телевизора изображение его лица.

Одновременно с записью на видеоманитофон динамики изменения термальных зон может осуществляться и звукозапись опроса. Последующий анализ речи опрашиваемого позволяет выявить дополнительные изменения эмоционального состояния объекта. Таким образом, речь идет о комплексном применении тепловизора и речевого сигнализатора психологического стресса.

3. Методические особенности использования полиграфных устройств при опросе

Еще в 1967 г. советскими учеными А.Р. Ратиновым и А.Н. Васильевым были высказаны предложения об использовании приборов типа «полиграф», но лишь при наличии бесконтактного контроля и только в оперативно-тактических целях. Использовать их следовало не для выводов о ложности или правдивости показаний виновности или невиновности, а для того, чтобы на основе научно

разработанной диагностики причастности установить, например, местонахождение трупа исчезнувшего человека, орудия преступления, похищенных вещей, что само по себе могло бы служить доказательствами по делу независимо от источников получения сведений.

Таким образом, речь идет о решении с помощью указанных устройств розыскных задач в целях установления традиционных вещественных доказательств, а их использование должно рассматриваться как применение специальной техники в оперативно-розыскной деятельности. Следовательно, правовой базой применения полиграфа является ст. 6 Федерального закона «Об оперативно-розыскной деятельности», определяющая в качестве одного из оперативно-розыскных мероприятий опрос граждан, в том числе с применением технических устройств.

Использование полиграфа при опросе представляет собой проводимую по специальным методикам беседу с опрашиваемым лицом с фиксацией его психофизиологических параметров (реакций) на задаваемые вопросы. Информация, полученная в ходе опроса, не может применяться в качестве доказательств, имеет вероятностный характер и только ориентирующее значение.

При необходимости проведения опроса с использованием полиграфа инициатор обращается с заданием в то подразделение правоохранительных органов, где имеется полиграфное устройство. Специалист предварительно знакомится с имеющимися материалами, изучает медицинские документы о состоянии здоровья опрашиваемого, консультируется при необходимости со специалистами медицинских учреждений, затем делает заключение о возможности (невозможности) опроса и определяет условия для его качественного проведения.

Опрос проводится только на основании задания и с письменного согласия опрашиваемого, в случае его отказа опрос с использованием полиграфа не проводится. Кроме того, опрашиваемый в любой момент вправе отказаться от дальнейшего проведения опроса и может быть ознакомлен с его результатами. Ознакомление осуществляет инициатор. При необходимости проводится повторный полиграфный опрос. Отказ от опроса не может рассматриваться в качестве подтверждения причастности опрашиваемого к совершению преступления и свидетельствовать о сокрытии известных ему сведений, а также вести к ущемлению его законных прав и свобод.

В процессе опроса задаются только те вопросы, которые предварительно согласованы с опрашиваемым. При этом они должны быть построены таким образом, чтобы исключалась возможность унижения чести и достоинства последнего. При таком опросе, с согласия опрашиваемого, можно проводить видео- или звукозапись.

Из-за вероятности получения необъективных результатов запрещается проводить опрос с использованием полиграфа в случаях:

- физического или психического истощения опрашиваемого;
- наличия у опрашиваемого психического заболевания или расстройства либо заболевания, связанного с нарушением сердечно-сосудистой или дыхательной системы;
- регулярного употребления опрашиваемым наркотических или сильнодействующих лекарственных препаратов;
- нахождения опрашиваемого в состоянии алкогольного или наркотического опьянения;
- наличия данных о беременности.

Собственно методическое обеспечение использования полиграфов при опросе граждан заключается в том, что вопросы, задаваемые испытуемому, условно можно поделить на три группы:

- нейтральные, не несущие эмоциональной нагрузки;
- контрольные, вызывающие эмоциональную нагрузку с прогнозируемым эффектом и являющиеся своего рода эталоном для последующего сравнения;
- проверочные, имеющие непосредственное отношение к расследуемому преступлению, но вызывающие эмоциональную реакцию только у причастного к нему лица, причем более сильную, чем при ответе на контрольный вопрос.

Все вопросы должны отвечать двум основным требованиям:

- быть предельно очевидны и ясны для опрашиваемого;
- обладать значительной силой эмоционального воздействия на виновного.

Существует три общих положения, вне зависимости от специфики уголовных дел, которых следует придерживаться, применяя полиграфные устройства:

- 1) обследование лучше всего проводить на начальном этапе следствия;
- 2) сразу после обследования, с учетом его результатов, целесообразно проведение допроса;
- 3) при расследовании дел, по которым в качестве предполагаемых причастных лиц проходят более пяти человек, во всех возможных случаях тестирование должно начинаться с «тестов максимального напряжения».

Так, например, методика применения устройств типа PSE в оперативно-розыскной деятельности заключается в следующем. Речь объекта опроса (подозреваемого в совершении преступления) вначале негласно контролируется с помощью анализатора голоса или записывается на магнитофон с целью последующего анализа. В процессе настройки прибора измеряется существующий на данный момент уровень эмоционального состояния, являющийся исходной точкой анализа. В этот период беседа ведется на заведомо нейтральные темы. Затем, при гласном применении аппаратуры, задаются вопросы или иным путем вводится информация, которая потенциально является психологическим раздражителем, но только для лица, причастного к данному правонарушению.

Если опрашиваемый не осведомлен о факте правонарушения, то для него такие сведения имеют нейтральный характер. К тому же как бы случайно

демонстрируются орудия совершения преступления, в беседе приводятся конкретные факты, имеющие прямое или косвенное отношение к деянию. При этом не используется информация, которая сама по себе может вызвать эмоциональное напряжение, например прямое обвинение в совершении преступления, а также фотографии трупа, оружие. По изменению уровня эмоционального состояния, в зависимости от совокупной характеристики динамики изменения контролируемых параметров речи, дается оценка степени реагирования, причем являющаяся результатом автоматизированной обработки данных анализа с помощью компьютера.

Дальнейший психологический анализ, в процессе которого сопоставляются уровень эмоционального стресса и содержание информации (как раздражителя), позволяет косвенно судить об уровне реакции на нее объекта опроса, выявлять неискренность, определять дальнейшее направление оперативно-розыскной работы.

В заключение приведем пример методики контрольно-проверочного теста, разработанной в лаборатории полиграфных испытаний полиции г. Чикаго (США). В ее основу положены двухтипные контрольно-проверочные вопросы, которые сравниваются с нейтральными. Нейтральные вопросы формулируются на основе известных для опрашиваемых данных. Разработчик методики – известный специалист в области проведения полиграфных испытаний Д. Рид.

По этой методике проверялся обвиняемый в убийстве Д. Джонса ранее судимый за кражу Й.Р. Браун. На каждый вопрос приведенных ниже тестов можно было отвечать только «да» или «нет». Пауза между ответами и вопросами составляла не более 15 секунд.

Тест:

1. Ваше имя?
2. Где Вы были ночью?
3. Вы знаете, кто убил Джонса?
4. Вы курите?
5. Вы застрелили Джонса ночью?
6. После освобождения Вы совершили новое преступление?
7. Вы находились ранее под стражей?
8. Приблизительно два месяца назад во время совершения квартирной кражи Вы убили (вымышленное имя), проживающего на улице (указывается известная испытуемому улица)?
9. Вы украли золотое кольцо у Джонса в прошлую субботу?
10. Вы присутствовали при убийстве Джонса?
11. Вы ответили правильно?

Рекомендации по применению теста:

1. Из всех вопросов приведенного теста 3-й является самым важным (проверочным). При виновности резко изменяются контролируемые параметры, прежде всего давление крови.

2. Вопрос 6-й является сравнительным. Если сравнивать реакции ответа на этот вопрос с аналогичными реакциями при ответе на вопросы, непосредственно связанные с расследуемым преступлением, то можно убедиться в невиновности или виновности человека.

3. Если опрашиваемый располагает достоверными данными о другом преступлении, которое ранее совершал подозреваемый, и предполагает, что он постарается скрыть правду, это служит исходной точкой фиксации на ложь.

Лекция 9. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

- 1. Понятие информационной безопасности.**
- 2. Факторы, влияющие на утечку информации.**
- 3. Методы и технические средства обеспечения безопасности информации.**
- 4. Рекомендации по организации защиты информации.**

1. Понятие информационной безопасности

Современные социально-экономические условия в России характеризуются общим ростом и ухудшением качественных характеристик преступности, возникновением и развитием новых форм преступных проявлений, оснащением криминальных структур новейшими техническими средствами, предназначенными для проведения как мероприятий разведывательного характера, так и информационных атак и психологического воздействия в каналах информационного обмена.

В настоящее время в целях дезорганизации деятельности правоохранительных органов криминалитетом разрабатываются системы несанкционированного съема, добывания, анализа и обработки оперативно-служебной информации. Задача правоохранительных органов состоит в организационном обеспечении своей практической деятельности посредством осуществления стратегических и тактических мер нейтрализации противодействия криминальных элементов силам правопорядка, следовательно, информация нуждается в защите, то есть в перекрытии каналов ее утечки.

По определению С.И. Ожегова, защита – то, что защищает, служит охраной. Защищать – значит охранять, ограждать от посягательств, враждебных действий, опасности.

Если информация рассматривается как объект защиты, ее принято классифицировать: а) по формам представления; б) имущественным правам; в)

категориям доступа. Информация может быть недокументированной (например, речевая) и документированной.

Содержание термина «информационная безопасность» определяется понятием «безопасность», которое в соответствии с Законом Российской Федерации «О безопасности» означает состояние защищенности жизненно важных интересов личности, общества и государства (ст. 1), а угроза безопасности – совокупность условий и факторов, создающих опасность для жизненно важных интересов личности и государства (ст. 3).

Таким образом, безопасность информации – обеспечение защиты информации от случайного или преднамеренного несанкционированного доступа к ней с целью раскрытия, изменения, уничтожения, использования в криминальных и иных целях.

Можно говорить о безопасности жизненно важных интересов личности, общества, государства в различных сферах деятельности, например экономической (экономическая безопасность), политической (политическая безопасность), военной (военная безопасность). Под информационной безопасностью понимается состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере (среде).

Основные угрозы жизненно важным интересам личности, общества, государства в информационной сфере можно разделить на три группы:

1. Угрозы воздействия недоброкачественной информации (недостоверной, ложной, дезинформации) на личность, общество, государство.

2. Угрозы несанкционированного и неправомерного воздействия посторонних лиц на информацию и информационные ресурсы (на производство информации, информационные ресурсы, системы их формирования и использования).

3. Угрозы информационным правам и свободам личности (праву на производство, распространение, поиск, получение, передачу и использование информации; праву на интеллектуальную собственность, на информацию и вещную собственность на документированную информацию; праву на личную тайну; праву на защиту чести и достоинства и т. п.).

Предотвращение и ликвидация угроз информационной безопасности личности, общества, государства основываются на разработке и реализации комплекса средств и механизмов защиты. Это могут быть организационные, технические, программные, социальные, правовые и иные механизмы, обеспечивающие локализацию и предотвращение таких угроз.

При создании и применении механизмов защиты возникают общественные отношения, связанные:

- с правом на защиту государства и общества от воздействия недостоверной, ложной информации;

- правом на защиту документированной информации, информационных ресурсов и продуктов как вещной собственности;

- правом на защиту информации и иных нематериальных объектов как интеллектуальной собственности;
- правом на защиту информационных систем, информационных технологий и средств их обеспечения как вещной собственности;
- правом на защиту личности в условиях информатизации;
- ограничением права на раскрытие личной тайны, а также иной информации ограниченного доступа без санкции ее собственника или владельца;
- обязанностями по защите государства и общества от вредного воздействия информации, защите самой информации, прав личности, тайны (личной, государственной, служебной и др.);
- ответственностью за нарушение прав и свобод личности, тайны и других ограничений доступа к информации, за компьютерные преступления.

Основными функциями системы безопасности в этом механизме являются:

- выявление и прогнозирование внутренних и внешних угроз жизненно важным интересам объектов безопасности, осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;
- создание и поддержание в готовности сил и средств обеспечения безопасности;
- управление силами и средствами обеспечения безопасности в повседневных условиях и при чрезвычайных ситуациях;
- осуществление системы мер по восстановлению нормального функционирования объектов безопасности в регионах, пострадавших в результате возникновения чрезвычайной ситуации;
- участие в мероприятиях по обеспечению безопасности за пределами Российской Федерации в соответствии с международными договорами и соглашениями, заключенными или признанными Российской Федерацией.

В соответствии с Доктриной информационной безопасности Российской Федерации к наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

- информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;
- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;
- информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами для этих объектов являются:

- разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности,

техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

- деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами для объектов являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и используемой для расследования преступлений;

- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

- отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного, справочного, криминалистического и статистического характера;

- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

- преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

2. Факторы, влияющие на утечку информации

С возникновением средств передачи информации стало возможным ее получение и использование заинтересованными субъектами, не являющимися непосредственно адресатами. Перехватывались и подменялись письма, посылались ложные сообщения. Шло время, были изобретены телефон, телеграф, фотокамера, радио. Чтобы справиться со стремительно нарастающим потоком информации, государственные и коммерческие структуры были вынуждены постоянно пополнять свой информационный арсенал разнообразными техническими средствами и системами, предназначенными для приема, передачи, обработки и хранения информации, а самые прогрессивные освоили высокие технологии и сферу телекоммуникаций.

Кто владеет информацией, тот владеет миром, отмечал У. Черчилль. Но он далеко не первым понял ценность информации.

Естественно, что и криминалитет стремится овладеть информацией, например о состоянии оперативной обстановки, работающих сотрудниках, и влиять с ее помощью на деятельность правоохранительных структур, направляет свои усилия на консолидацию противоправной деятельности, подкуп должностных лиц правоохранительных и государственных органов исполнительной и законодательной власти. Негативные процессы, происходящие в криминальной среде, приобретают структурно организованные формы.

Бурное развитие техники, технологии, информатики в последние десятилетия вызвало стремительное развитие технических устройств и систем разведки. В самом деле, слишком часто оказывалось выгоднее потратить какую-то сумму на добывание уже существующей технологии, чем в несколько раз большую на создание собственной. А в политике или военном деле выигрыш в результате владения информацией иногда бывает просто бесценным.

В настоящее время развитие электроники позволило достичь значительного прогресса в разработке и применении разнообразных средств технического проникновения в личную жизнь человека или в его конфиденциальную информацию. Во всех развитых странах в создание устройств и систем ведения технической разведки вкладываются огромные средства. Сотни фирм во многих государствах активно работают в этой области, серийно производятся десятки тысяч моделей «шпионской» техники. Подобные устройства так легко установить и сложно обнаружить, что их вероятные жертвы – коммерсанты, преступники или крупные руководители – редко могут быть абсолютно уверенными, что их разговоры не прослушиваются или не записываются.

Аппаратура стала портативной, высоконадежной и нередко имеет практически неограниченный срок службы. Размещенная в часах или шариковой ручке, стакане или цветочном горшке, она устанавливается в кабинете, приемной для посетителей, спальне или автомобиле – и все разговоры можно прослушивать с достаточно большого расстояния. В последние годы появились устройства, размер которых не превышает 10–15 мм. Они накапливают и передают сигналы по сверхтонким проводникам, вплетаемым в ковры или драпировки, по волоконно-оптическим кабелям или эфиру. При этом используются различные способы передачи информации. Широко применяется дистанционное включение, а также системы с накоплением и последующей передачей сигналов кратковременными зашифрованными сериями. Кроме того, разработаны устройства, которые могут записать перехваченную информацию, хранить ее в течение суток или недели, передать в быстродействующем режиме за миллисекунду, стереть запись и начать процесс снова.

В середине 80-х годов появились изделия, передающие информацию по кабелям электропитания технических средств, в которые они могут быть оперативно вмонтированы. Эта информация может регистрироваться практически в любой части здания и даже за его пределами. Применяются и миниатюрные микрофоны, присоединяемые к металлическим элементам конструкций контролируемого помещения и обнаруживаемые только с помощью рентгеновской аппаратуры. Существуют и полностью пассивные устройства, не содержащие электронных компонентов: небольшие коробочки с точно подобранными линейными размерами, которые отражают направленные радиосигналы определенной частоты. Под воздействием акустических волн они вибрируют и модулируют отраженные волны.

В качестве примера можно привести самый маленький и самый дорогой в мире радиомикрофон, габариты которого не превышают четверти карандашной стиральной резинки. Этот миниатюрный передатчик питается от изотопного элемента и способен в течение года воспринимать и передавать на приемное устройство, расположенное от него на расстоянии до полутора километров, разговор, который ведется в помещении шепотом.

Таким образом, одной из угроз деятельности различных объектов является несанкционированный съем циркулирующей в них информации – служебной, коммерческой, личной и, что в настоящее время особенно актуально, обрабатываемой различными техническими средствами.

Естественно, ценность информации, добываемой путем негласной установки аппаратуры, определяет и масштабы операции. Они приобретают большой размах в странах, где разведывательные органы нацелены на поддержку государственных и коммерческих структур в борьбе с их конкурентами.

Нередко сотрудники разведывательных органов поставляют частным фирмам информацию, полученную оперативным путем.

Что касается фактора преступности, то, как отмечалось ранее, организованные и многонациональные преступные сообщества все в больших масштабах используют технические средства для поддержки своей деятельности. Они прослушивают юридические фирмы, правоохранительные органы, финансовые организации, потенциальных жертв похищения с целью грабежа, вымогательства и шантажа и другие интересующие их объекты.

В отношении фактора, связанного с характером конфиденциальной информации, можно утверждать, что, по признанию специалистов, определенные секторы производства и государственные структуры подвержены большему риску прослушивания, чем другие (бизнес, связанный с ценными изделиями, когда заключаются контракты на многие миллионы долларов, оборонная промышленность, компании по производству лекарств и наркотиков, военные и властные структуры и т. д.).

Рассматривая фактор потери конфиденциальной информации, связанный с простотой (сложностью) установки и снятия технических устройств контроля, еще раз отметим, что развитие научно-технического прогресса привело к тому, что электронные приборы снятия информации в настоящее время можно приобрести в любой стране мира. Совершенная аппаратура может использоваться для прослушивания обсуждения различных вопросов оперативно-служебной деятельности.

Интерес к темным сторонам жизни знаменитых людей и организаций нередко заставляет и средства массовой информации (СМИ) использовать прослушивание. Люди, близкие к СМИ, применяют специальные приборы для получения интересующих сведений, иногда в целях последующей продажи. Достижения научно-технического прогресса способствуют негласному проникновению в личную и общественную жизнь граждан и организаций.

Следовательно, при отсутствии должного внимания к защите информации она может попасть к посторонним лицам.

Немаловажным является и личностный фактор утечки информации в учреждениях и органах уголовно-исполнительной системы, учитывающий такие влияющие на совершение различного рода преступлений характерные особенности человека, как скаредность, невежество, нецивилизованность, ротозейство.

Необходимо упомянуть и о влиянии на утечку информации таких факторов, как шантаж и запугивание.

С учетом изложенного к основным факторам, обуславливающим защиту информации в правоохранительных органах, можно отнести следующие:

- социально-экономические условия в стране и обществе, характеризующиеся ростом и ухудшением качественных характеристик преступности, возникновением и развитием новых форм криминальных проявлений;

- личностный (человеческий, общегражданский) фактор, обусловленный тем, что такие понятия, как «информационная война» и «информационное оружие», в настоящее время наполняются новым смыслом и становятся привычными не только в столкновении противоборствующих политических сил, но и в противостоянии правоохранительных органов и преступного мира;

- оперативно-режимный (документальный) фактор, зависящий от наличия документов, составляющих государственную и служебную тайну;

- технический (технологический) фактор, связанный с оснащением криминальных структур современными техническими средствами и использованием новых технологий обработки информации для достижения корыстных целей, извлечения максимальной выгоды из противозаконной деятельности, в том числе проведения информационных и психологических атак;

- организационный фактор, выражающийся в несовершенстве и отсутствии единой системы методического обеспечения проведения защитных мероприятий, так как большинство авторов уделяют основное внимание технической стороне этой проблемы;

- нормативно-правовой, представляющий собой некоторое несовершенство законодательной и правовой базы по защите информации от несанкционированного доступа, съема и искажения, а также обусловленный в ряде случаев недостаточными знаниями и игнорированием сотрудниками требований соблюдения норм и правил режима секретности.

3. Методы и технические средства обеспечения безопасности информации

Каждый метод получения информации должен быть обеспечен методами ее защиты. Обеспечение защиты информации зависит: от компетентности в вопросах защиты информации лиц, которым это дело поручено; наличия соответствующего оборудования, необходимого для проведения мероприятий по защите. Наиболее важным является первое, так как очевидно, что самая совершенная аппаратура не принесет положительных результатов без профессиональной интеллектуальной деятельности сотрудников уголовно-исполнительной системы.

Рассматривая методы защиты информации в учреждениях и органах уголовно-исполнительной системы, необходимо отметить, что в настоящее время имеются большие возможности по ее несанкционированному съему, особенно с помощью прослушивания телефонных переговоров. Следовательно, при отсутствии должного внимания к защите каналов связи важная информация может стать достоянием злоумышленников.

Учитывая изложенное, отметим, что эффективная защита в уголовно-исполнительной системе конфиденциальной информации возможна лишь при условии, если соответствующие мероприятия будут носить всесторонний и непрерывный характер. Это достигается осуществлением совокупности мер по ее защите в ходе всего процесса подготовки, обсуждения, обработки, передачи и хранения такой информации.

Защита информации в целом представляет собой комплекс мероприятий организационного и технического характера. Методы защиты информации полностью зависят от факторов, обуславливающих их. К методам защиты информации можно отнести следующие:

- организационный, связанный с выработкой и применением конкретных методик проведения мероприятий по предотвращению утечки конфиденциальной информации;
- нормативно-правовой, опирающийся на соблюдение требований нормативных и правовых актов по хранению конфиденциальной информации;
- личностный, обусловленный морально-психологическими характеристиками конкретного лица;
- физический, связанный с расположением и устройством помещения или местности, где циркулирует конфиденциальная информация;
- технический, зависящий от наличия специальной техники и технологий защиты информации и владения сотрудниками навыками в их применении.

Основанием для проведения защитных мероприятий могут стать сведения об утечке информации, обсуждающиеся в конкретном помещении или обрабатываемые на конкретном техническом средстве.

Проводя мероприятия по защите от несанкционированного доступа к информации, не следует стремиться обеспечить защиту всего здания от технического проникновения. Главное – ограничить доступ в те места и к той технике, где сосредоточена конфиденциальная информация. Использование качественных замков, средств сигнализации, хорошая звукоизоляция стен, дверей, потолков и пола, звуковая защита вентиляционных каналов, отверстий и труб, проходящих через эти помещения, демонтаж излишней проводки, а также применение специальных устройств защиты в существенной мере затруднят или сделают бессмысленными попытки внедрения специальной техники съема информации.

Необходимо применять и личностный метод защиты, так как специфика деятельности правоохранительных органов выдвигает ряд требований к поведению сотрудников, особенно, на наш взгляд, это касается сотрудников оперативных служб.

Рассматривая технический аспект защиты информации, нужно отметить тот факт, что ряд преступлений можно было бы предотвратить, если бы своевременно были приняты меры превентивного характера, исключающие техническое проникновение к конфиденциальной информации.

Во многих организациях, действующих на территории Российской Федерации, большое внимание уделяется вопросам сохранения государственной и служебной (коммерческой) тайны. Однако недостаток сведений о возможностях технических средств разведки, простота получения с их помощью нужной информации нередко делают возможным беспрепятственный доступ к информации, нуждающейся в защите.

Надо иметь в виду, что для гарантированной защиты применение технических средств должно быть как можно более комплексным и, кроме того, обязательно сочетаться с мероприятиями организационного характера.

Организация технических мероприятий включает: поиск и уничтожение технических средств разведки; кодирование информации или передаваемого сигнала; подавление технических средств постановкой помехи; мероприятия пассивной защиты: экранирование, развязки, заземление, звукоизоляция и т. д.; применение систем ограничения доступа, в том числе биометрических систем опознавания личности.

Напомним, что утечка информации в общем виде рассматривается как непреднамеренная передача секретной информации по некоторой побочной системе связи. В классических (традиционных) системах передающая сторона заинтересована в возможно большем ухудшении передачи побочной информации, что способствует ее защите. Также в реальных условиях в окружающем пространстве присутствуют многочисленные помехи как естественного, так и искусственного происхождения, которые существенным образом влияют на возможность приема. Поэтому технические каналы утечки информации чаще всего рассматриваются в совокупности с источниками

помех. На традиционные системы связи такие помехи оказывают негативное влияние, в значительной степени затрудняющее прием, однако для защиты технических средств от утечки информации по побочным каналам эти помехи оказываются полезными и нередко создаются специально, что является одним из средств обеспечения защиты информации.

Наибольших усилий требуют организационные мероприятия по поиску технических средств дистанционного съема информации. Применяется обычный физический поиск и поиск с помощью специальных технических средств, такой как обнаружение опасных излучений с помощью радиоэлектронной аппаратуры перехвата.

Во время проведения мероприятий в актовом залах, других значительных по размерам помещениях при передаче информации по линиям связи могут применяться зашумляющие генераторы – акустические генераторы шума. Они защищают условные поверхности помещения от действия радиотехнических, лазерных, акустических и других средств, а некоторые из них позволяют производить защищенное звукоусиление при озвучивании залов и других помещений на 50–250 мест при проведении закрытых мероприятий.

Для обнаружения «опасных» электромагнитных излучений и измерения их уровня применяются специальные приемники, автоматически сканирующие по диапазону. С их помощью осуществляется поиск и фиксация рабочих частот, определяется местонахождение радиозакладок, включенных в момент поиска. Для выявления радиозакладок, выключенных в момент поиска и не излучающих сигналы, по которым их можно обнаружить радиоприемной аппаратурой, а также для поиска спрятанных микрофонных систем и миниатюрных магнитофонов применяются специальная рентгеновская аппаратура, нелинейные детекторы, имеющие встроенные генераторы микроволновых колебаний и устройства приема и анализа их отклика, реагирующие на наличие в зоне поиска полупроводниковых элементов, подобно тому как металлоискатели реагируют на присутствие металла.

Наиболее сложными и дорогостоящими средствами дистанционного перехвата речи из помещений являются лазерные устройства. Один из достаточно простых, но очень эффективных способов защиты от лазерных устройств заключается в том, чтобы с помощью специальных устройств сделать амплитуду вибрации стекла много большей, чем вызванную голосом человека. При этом на приемной стороне возникают трудности в детектировании речевого сигнала.

Кроме перечисленных, в системах защиты информации используются и многие другие устройства и приборы, например: сетевые фильтры, исключающие возможность утечки информации по цепям электропитания; приборы, обеспечивающие автоматическую запись телефонных разговоров; рассмотренные ранее акустические генераторы шума, маскирующие звуковой сигнал, и многие другие.

Для защиты телефонных и радиопереговоров могут использоваться скремблеры, осуществляющие стойкие алгоритмы шифрования речевых сообщений. При этом для ведения переговоров необходимо два таких устройства. Связавшись с имеющим подобное устройство абонентом, вы договариваетесь о переходе на закрытую связь и осуществляете ее через эти устройства, которые подключены, например, путем соответствующих замен телефонных трубок.

В последнее время стали выпускаться аппаратные и программные средства, позволяющие криптографически защищать системы передачи данных, использующие в качестве элемента канала связи телефонные и радиолинии, то есть радиостанции, телетайпы, телефаксы, ПК и др. Применяются и выжигатели телефонных закладок, установленных параллельным или последовательным способом, которые при подключении к телефонной линии выводят из строя аппаратуру прослушивания, не нарушая работы телефонной сети.

В качестве защиты источников конфиденциальной информации от несанкционированного доступа используется видео- и фототехника. Системы фототехники применяются для фотосъемки посетителей административных зданий, режимных учреждений и т. п. Такие системы можно условно разделить: на системы скрытой охраны, которые обнаружить без специальной техники невозможно; системы открытого наблюдения, применение которых очевидно; отпугивающие системы.

Скрытые системы наблюдения имеют то преимущество, что с их помощью можно следить за поведением людей (сотрудников, посетителей и т.д.) в обстановке, когда они остаются в помещении одни. Это может оказать помощь в выявлении источников утечки информации.

Системы открытого наблюдения применяются тогда, когда не нужно скрывать факт наблюдения. В этом случае наличие видеокамеры сдерживает потенциального вредителя от неправомерных действий.

Отпугивающие системы предназначены для имитации систем охраны помещений, то есть это точно выполненные макеты видеокамер.

С развитием информационных технологий, широким внедрением в повседневную жизнь персональных компьютеров обостряется проблема защиты информации, обрабатываемой с их помощью. В системе защиты персональных компьютеров используются различные программные и аппаратные методы, которые значительно расширяют возможности по обеспечению безопасности хранящейся информации.

4. Рекомендации по организации защиты информации

Процесс подготовки и проведения защитных мероприятий складывается из последовательных действий (этапов): 1) постановка задач поиска; 2) оценка системы защиты объекта; 3) контроль окружения объекта; 4) визуальный осмотр

объекта; 5) проверка электронной техники; 6) проверка мебели, интерьера; 7) проверка коммуникаций; 8) проверка ограждающих конструкций; 9) подготовка отчетной документации.

Прежде всего рекомендуется точно оценить опасность несанкционированного съема информации. Начните с того, что определите ценность информации, на которую будет нацелена операция злоумышленника, и ответьте на следующие вопросы. Какие убытки вы потерпите, если он получит конфиденциальную информацию? Сколько будет стоить ему добывание ваших сведений? Какие выгоды он получит, если ему станет доступна ваша конфиденциальная информация? Каковы возможности злоумышленника? Соответствует ли ваша оборона той опасности, которая может исходить от ваших конкурентов?

Определив степень опасности, необходимо постараться сделать следующее:

1. Избежать опасности путем изменения местонахождения вашего рабочего помещения.

2. Обезопасить себя от средств съема информации, шифруя разговоры, используя при этом звуконепроницаемые стеклянные барьеры в нужных местах, маскирование разговоров с помощью шумов, постоянное контрнаблюдение, установку телефонов с шифрующим устройством, передачу дезинформации для обнаружения прослушивания, применение криптографической аппаратуры, строгие меры общей безопасности.

3. Воспринять утечку информации и особенно прослушивание переговоров как должное и предпринять ответные действия.

Комплексная задача по обнаружению и ликвидации угрозы съема информации решается в процессе проведения поисковых мероприятий. Необходимо определить состояние технической безопасности объекта, его помещений, подготовить и принять меры, исключающие возможность утечки информации в дальнейшем.

Нет смысла тратить средства, если через некоторое время после проведения поискового мероприятия кто-то снова сможет занести в помещение и установить аппаратуру съема информации. Поисковое мероприятие будет эффективно только при поддержании соответствующего режима безопасности и выполнении рекомендуемых мер защиты.

Отметим, что техника съема информации не может появиться на объекте сама по себе: ее должен кто-то принести и установить. Для этих целей нередко используют сотрудников объекта (или лиц, его посещающих), например монтера-телефониста, электрика, уборщицу, плотника. Люди этих специальностей периодически работают в кабинетах, где ведутся разговоры, хранятся и обрабатывается разнообразная информация, и имеют достаточно времени для тщательного изучения помещения и подбора мест установки спецтехники для дистанционного съема информации, проверки эффективности ее работы, замены элементов электропитания и демонтажа после окончания работы.

Перед проведением важного совещания, переговоров или беседы на рабочем столе может быть подменен какой-либо предмет на точно такой же, но с электронной «начинкой», а затем возвращен на место. Спецтехника может быть спрятана в подарках, сувенирах, которыми часто украшают кабинеты и другие помещения, где ведутся переговоры.

Наиболее удобная ситуация для внедрения разнообразной техники – проведение капитального или косметического ремонта.

Так как классическим местом для размещения техники прослушивания переговоров, ведущихся в помещении, является телефон, в кабинетах, где проводятся конфиденциальные беседы, лучше устанавливать только те телефоны, которые рекомендованы специалистами по радиоэлектронной защите информации и предварительно ими проверены.

Чтобы капитально установить спецтехнику в ограждающих конструкциях (стены, пол, потолок), необходимо располагать достаточно большой (3–5 человек) технически подготовленной бригадой, возможностью конспиративного захода на объект и в помещение хотя бы на несколько часов. В то же время, например, радиозакладку может внедрить и неспециалист во время одного кратковременного проникновения в помещение.

Следует учесть, что аппаратуру со сложными системами кодирования и передачи информации рядовому гражданину приобрести абсолютно невозможно. Она изготавливается только по заказу спецслужб и строго учитывается, дорого стоит.

Иногда проводится специальная защита помещений методом экранирования с использованием таких материалов, как листовая сталь, проводящая медная сетка с ячейкой 2,5 мм или алюминиевая фольга. Экранированию подвергается все помещение: полы, стены, потолки, двери.

Выбирается одна наиболее удобно расположенная комната, желательно не имеющая стен, смежных с неконтролируемыми помещениями, а также без вентиляционных отверстий. На пол, например под линолеум, укладывается фольга, сетка, стены под обоями или панелями также покрываются фольгой. Потолки можно сделать алюминиевыми подвесными, а на окнах использовать алюминиевые жалюзи, специальные проводящие стекла или проводящие (из ткани с омедненной нитью) шторы. При этом не следует забывать о дверях. Необходимо обеспечить электрический контакт экранов пола, потолка, стен по всему периметру помещения.

При проведении работ по экранированию целесообразно произвести и звукоизоляцию помещения, которая уменьшит вероятность прослушивания через стены, потолки, полы акустическими средствами съема информации. Эффективным звукоизолирующим материалом является пенопласт: слой пенопласта толщиной 50 мм равен по звукоизоляции бетонной стене толщиной 50 см.

Таким образом, мы выяснили, что защита информации правоохранительных органов – довольно широкомасштабная программа. Защиту информации с помощью технических средств можно классифицировать на физическую и аппаратную.

Физическая защита информации предусматривает использование качественных замков, средств сигнализации, хорошую звукоизоляцию стен, дверей, потолков и пола, звуковую защиту вентиляционных каналов, отверстий и труб, проходящих через помещения, демонтаж излишней проводки и тому подобные действия.

Аппаратная защита информации – комплекс механических, электромеханических, электронных, оптических, лазерных, радиотехнических, радиоэлектронных, радиолокационных и других устройств, систем и сооружений, предназначенных для защиты информации от несанкционированного доступа, копирования, кражи или модификации.

К техническим средствам защиты информации в правоохранительных органах относятся: организационные, технические, криптографические, программные и другие, предназначенные для защиты конфиденциальных сведений¹.

В заключение отметим, что решение вопросов обеспечения защиты информации возможно только при комплексном подходе к этой проблеме. И любая самая совершенная техника в руках дилетанта окажется ненужной игрушкой без соответствующих навыков в ее применении и знания организационных и правовых основ этой деятельности.

Лекция 10. ОСНОВЫ ОРГАНИЗАЦИИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ

1. Компьютерные преступления, их общая криминалистическая характеристика и важнейшие факторы, влияющие на компьютерную безопасность.

2. Основные методы обеспечения компьютерной безопасности.

1. Компьютерные преступления, их общая криминалистическая характеристика и важнейшие факторы, влияющие на компьютерную безопасность

С появлением современных средств вычислительной техники и телекоммуникаций традиционные преступления – воровство, мошенничество, шпионаж, вымогательство – трансформировались в новые формы. Кроме того, появились специфические для компьютерных систем и сетей преступления. Намечается тенденция к использованию информационных технологий организованными преступными группами и распространение их деятельности на межгосударственный уровень. Сотрудники правоохранительных органов при раскрытии и расследовании компьютерных преступлений неизбежно сталкиваются с большими трудностями, так как преступления в сфере компьютерной обработки информации характеризуются скрытностью, трудностями сбора улик по установлению фактов их совершения, сложностью доказывания в суде. Субъекты преступлений – это, как правило, высококвалифицированные программисты, инженеры, специалисты в области телекоммуникационных систем, банковские работники, бывшие сотрудники спецслужб.

Есть основания утверждать, что при переходе цивилизации к информационному обществу все большее количество преступлений будет совершаться в информационной сфере. Мировое сообщество крайне озабочено состоянием защиты национальных информационных ресурсов в связи с расширением доступа к ним через различные открытые информационные сети.

Под информационной системой понимают организованную совокупность информационных технологий, объектов и отношений между ними, образующую единое целое.

Под автоматизированной системой обработки информации принято понимать организационно-техническую систему, состоящую из следующих взаимосвязанных элементов:

- средства вычислительной техники и связи;
- программное обеспечение;

- информация, хранящаяся на различных носителях;
- персонал и пользователи системы.

Интерес к вопросам сохранности компьютерной информации, защиты ее от случайного и преднамеренного уничтожения, повреждения и несанкционированного получения появился, когда ПК стали широко применяться в экономической, социально-политической и оборонной областях. В автоматизированных системах можно скрытно получить доступ к информационным архивам, которые концентрируются в одном месте в больших объемах. Кроме того, появилась возможность дистанционного получения информации через терминалы. Поэтому для ее защиты требуются принципиально новые методы и средства, разработанные с учетом ценности информации, условий работы, технических и программных возможностей ПК и других средств сбора, передачи и обработки данных.

Несанкционированным доступом к информации персонального компьютера будем называть незапланированное ознакомление, обработку, копирование, применение различных вирусов, в том числе разрушающих программные продукты, а также модификацию или уничтожение информации в нарушение установленных правил разграничения доступа.

Для успешной борьбы с подобным видом преступной деятельности следует тщательно изучать ее особенности, хорошо знать виды неправомерного доступа к информации, создания и использования вредоносных программ для ПК в сетях телекоммуникаций и т. д.

Надо также иметь в виду, что современные системы связи (сотовые, транковые, проводные на основе АТС, радиотелефонные удлинители и др.) рассматриваются не только как собственно системы связи, но и как ПК или составляющие элементы системы ПК, то есть как телекоммуникационные системы, к которым, например, можно отнести:

- отдельные составляющие систем связи – как периферийные устройства ПК, системы ПК (сотовый телефон, базовая станция сотовой или транковой сети, радиотелефонный удлинитель, процессор электронной АТС и т. д.);
- носители информации управляющего компьютера сотовой системы, ПЗУ или РТС-контроллер в сотовой или трубке радиоудлинителя – как носители компьютерной информации на машинных носителях;
- программы функционирования управляющих компьютеров систем связи (управляющего компьютера сотовой системы), процессоров сотовых телефонов или радиотелефонных удлинителей – как компьютерные программы;
- телефонные номера, коды доступа, идентификации абонента, сигналы управления и сигнализации (сигналы запроса аппаратуры автоматического определения телефонного номера) – как компьютерная информация.

Таким образом, стандартность архитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, высокая мобильность программного обеспечения и ряд других признаков

определяют сравнительно легкий доступ профессионала к информации, находящейся в ПК. Если персональным компьютером пользуется группа пользователей, то может возникнуть необходимость в ограничении доступа к информации различных потребителей.

Элементами криминалистической характеристики компьютерных преступлений (по Р.С. Белкину) являются: типичные следственные ситуации; характеристика личности преступника; способ совершения преступления; обстановка преступления; типичные материальные следы преступления; способ сокрытия преступления.

Итак, под криминалистической характеристикой компьютерных преступлений будем понимать совокупность наиболее характерной, криминалистически значимой взаимосвязанной информации о признаках и свойствах такого рода преступлений, способную служить основанием для выдвижения версий о событии преступления и личности преступника, позволяющую верно оценить ситуации, возникающие в процессе раскрытия и расследования компьютерных преступлений, обуславливающую применение соответствующих криминалистических методов, приемов и средств.

Следовательно, криминалистическая характеристика компьютерных преступлений включает в себя: способы совершения, особенности непосредственного предмета преступного посягательства, особенности следовой информации, личностную характеристику преступника, особенности обстановки совершения преступления (место, время и др.).

В связи с происходящими изменениями в области информатизации определение предмета преступного посягательства требует нового научного подхода, то есть предметом преступления в контексте данного явления будет информация в виде программных средств и файлов данных.

Следует отметить, что вероятность несанкционированного доступа к системе возрастает при ее перегрузках, которые возникают, например, при массовом подключении к ней пользователей (в начале рабочего дня). Так, нарушители способны создать сходную ситуацию, направляя в систему поток сообщений, которые она не в состоянии корректно обработать. В результате создается открытый канал передачи данных, через который возможен несанкционированный доступ. Под каналом передачи данных при этом понимаются средства двустороннего обмена данными, представляющие собой совокупность аппаратуры окончания канала данных и линии передачи данных.

В криминалистике способ совершения преступления представляет собой систему взаимообусловленных, подвижно детерминированных действий, направленных на подготовку, совершение и сокрытие преступления, связанных с использованием соответствующих орудий и средств, а также времени, места и других способствующих обстоятельств объективной обстановки совершения преступления.

В литературе описывается множество способов совершения компьютерных преступлений в зависимости от классификации информации, вида машинных носителей, подключения или неподключения к сети и т. д. Так, рабочей группой Интерпола в 1991 г. разработан и встроен в автоматизированную поисковую систему запросов следующий классификатор компьютерных преступлений:

Каждая группа, в свою очередь, разбита на подгруппы:

QA

QAN – «компьютерный абордаж» (хакинг): несанкционированный доступ в компьютер или компьютерную сеть;

QAI – перехват: несанкционированный перехват информации при помощи технических средств, несанкционированные обращения в компьютерную систему или сеть как из нее, так и внутри компьютерной системы или сети;

QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты;

QAZ – прочие виды несанкционированного доступа и перехвата.

QD

QDL – «логическая бомба»: неправомерное изменение компьютерных данных путем внедрения «логической бомбы»;

QDT – «троянский конь»: неправомерное изменение компьютерных данных путем внедрения «троянского коня»;

QDV – вирус: изменение компьютерных данных путем внедрения или распространения компьютерного вируса;

QDW – «червь»: несанкционированное изменение компьютерных данных или программ путем передачи, внедрения или распространения компьютерного «червя» в компьютерной сети;

QDZ – прочие виды изменения данных.

QF

QFC – компьютерные мошенничества с банкоматами, связанные с хищением из них наличных денег;

QFF – компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и т. д.);

QFG – мошенничества и хищения, связанные с игровыми автоматами;

QFM – манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода в компьютерные системы или вывода из них путем манипуляции программами;

QFP – компьютерные мошенничества и хищения, связанные с платежными средствами;

QFT – телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы;

QFZ – прочие компьютерные мошенничества.

QR

QRG/QRS – незаконное копирование, распространение или опубликование компьютерных игр и другого програм-ного обеспечения;

QRT – незаконное копирование защищенной законом топографии полупроводниковых изделий; незаконная коммерческая эксплуатация либо импорт с этой целью топографии или самого полупроводникового изделия, произведенного с использованием данной топографии;

QRZ – прочее незаконное копирование.

QS

QSH – саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ либо вмешательство в работу компьютерных систем с намерением нарушить функционирование компьютерной (телекоммуникационной) системы;

QSS – компьютерный саботаж программы: несанкционированное стирание, повреждение, ухудшение или подавление компьютерных данных или программ;

QSZ – прочие виды саботажа.

QZ

QZB – электронные доски объявлений (BBS): использование BBS для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;

QZE – хищение информации, представляющей собой коммерческую тайну (компьютерный шпионаж): приобретение незаконными средствами или передача информации, представляющей собой коммерческую тайну, с намерением причинить экономический ущерб или получить незаконные экономические преимущества;

QZS – материал конфиденциального характера: использование компьютерных сетей или систем для хранения, обмена, распространения или перемещения информации конфиденциального характера;

QZZ – прочие компьютерные преступления.

Ссылаясь на Уголовный кодекс Российской Федерации, ученые подразделяют личности компьютерных преступников на несколько категорий, куда входят лица:

- осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой;
- осуществляющие неправомерный доступ к компьютерной информации с использованием своего служебного положения;
- имеющие доступ к ПК, но осуществляющие неправомерный доступ к компьютерной информации или нарушающие правила эксплуатации ПК;
- создающие, использующие и распространяющие вредоносные программы.

Исследователи также выделяют следующие типы компьютерных преступников:

- лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с

элементами своеобразного фанатизма и изобретательности (так называемые хакеры и крекеры);

- лица, страдающие новой разновидностью психической неполноценности – информационными болезнями или компьютерными фобиями (игроманы; работающие за компьютером длительное время; страдающие информационными перегрузками и т. д.);

- профессиональные компьютерные преступники с ярко выраженными корыстными целями.

К наиболее опасным преступникам ученые относят хакеров и крекеров.

Хакеры – компьютерные хулиганы, проникающие в память чужих компьютеров с помощью своих, подключенных по телефонным каналам к сетям передачи данных. При этом преследуются разнообразные цели: от любопытства и удовлетворения тщеславия до получения конкретной выгоды. Одним из основных внешнеповеденческих отличительных признаков хакерства является безразличие ко всему, что не имеет непосредственного отношения к работе с компьютером. У хакеров атрофирована установка на конечный результат, их не интересует полезность и возможность передачи продукта их деятельности в общественное пользование. Вследствие этого они игнорируют общественные интересы и проявляют «компьютерный снобизм». Для хакеров характерна симптоматика бегства от реальности.

Под внешнеповеденческими признаками лиц, обладающих общим для них отличительным признаком, понимается совокупность признаков внешности человека (анатомических, функциональных), речевых свойств, эмоциональных признаков, выраженных индивидуально-типологических особенностей (темперамент, характер).

Мотивы поступков различны, как правило, это хулиганские побуждения, реже – исследовательский интерес.

Крекеры – компьютерные «террористы», создающие программы-вирусы и специализирующиеся на проникновении в компьютерные сети и системы с целью овладения конфиденциальной информацией. Являясь программистами очень высокого класса (в отличие от хакеров), они могут стереть или изменить данные в соответствии со своими интересами. В социальном плане крекеры инфантильны, безответственны.

Мотивами поступков крекеров может быть мщение за нанесенную им обиду, попытка дезорганизовать вычислительные системы своих конкурентов или авторская защита программных продуктов от несанкционированного копирования и распространения.

Общими признаками для указанных подгрупп являются:

- завышенная оценка своих профессиональных и, как следствие, интеллектуальных способностей;

- использование специфического жаргона не только в кругу специалистов, но и при повседневном общении;

- отсутствие интереса к обычной жизни и др.

Для рассмотренных подгрупп следует указать особенности, свидетельствующие о совершении компьютерного преступления лицами, входящими в них:

- отсутствие целеустремленной, продуманной подготовки к преступлению;
- оригинальность способа совершения преступления;
- непринятие мер к сокрытию преступления;
- совершение на месте происшествия действий, которые условно можно назвать озорными, выходящими за рамки принятых норм.

Под обстановкой совершения преступления понимают систему различного рода взаимодействующих между собой объектов, явлений и процессов, характеризующих условия места и времени, вещественные, физико-химические, метеорологические и иные условия окружающей среды, производственные факторы, особенности поведения участников события, не имеющих прямого отношения к нему, и другие обстоятельства объективной реальности, сложившиеся (независимо или по воле участников) в момент преступления, влияющие на способ его совершения и проявляющиеся в следах, позволяющих судить об особенностях этой системы и содержании преступного события.

Способ совершения компьютерного преступления будет определяться наиболее характерными составляющими обстановки:

- местом и временем действия преступника (преступников);
- особенностью компьютеризации субъекта хозяйствования;
- особенностями организации информационной безопасности;
- возможностями нарушения целостности компьютерной информации без непосредственного участия человека;
- уровнем квалификации специалистов, обеспечивающих защиту информации, а также администрирование компьютеров и их сетей.

Рассматривая важнейшие факторы, влияющие на компьютерную безопасность, обратимся к Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 9 сентября 2000 г., где определены следующие угрозы информационной безопасности информационных и телекоммуникационных систем, а именно:

- противоправный сбор и использование информации;
- нарушение технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникаций и связи;

- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технических средствах обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от форм собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на каналах связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникаций и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Под доступом к информации в нашем случае будем понимать ознакомление с информацией или получение возможности ее обработки.

Под угрозой следует понимать реально существующую либо потенциальную опасность случайного или умышленного нарушения информационной безопасности. Это обстоятельства или события, которые могут явиться причиной нанесения ущерба интересам личности, общества или государства.

Раскрывая направления деятельности по обеспечению информационной безопасности, ряд авторов предлагают различное толкование информационных угроз в зависимости от факторов, влияющих на защиту информации. К ним, например, относятся: интересы государства и общества, экономические, организационно-технические факторы, которые, в свою очередь, группируются в глобальные, региональные и локальные факторы угроз.

Таким образом, обобщенный перечень угроз информационной компьютерной безопасности включает в себя следующие группы факторов:

1. Антропогенные угрозы (противозаконная деятельность криминальных структур, нарушителей, недобросовестных партнеров, конкурентов, отдельных работников организаций и т. п.).
2. Техногенные угрозы (некачественное оборудование, программное обеспечение и средства защиты, средства связи, охраны, сигнализации, иные применяемые технические средства, а также опасные производства, транспорт и т. д.).
3. Стихийные угрозы (землетрясения, цунами, затопления, ураганы, иные природные явления).

Необходимо отметить, что есть два вида несанкционированного доступа к услугам телекоммуникационных сетей – технологический и административный.

Технологический характеризуется использованием нелегальными абонентами технического оборудования, аналогичного работающему в системе связи. Такая аппаратура опознается как существующий абонент со всеми вытекающими последствиями, например, по оплате услуг, когда абоненту системы приходится оплачивать временной ресурс, потраченный нелегальным абонентом. Иногда несанкционированный доступ происходит без идентификации абонента, путем технологического «обмана» аппаратуры.

Административный доступ характеризуется использованием ресурсов телекоммуникационной системы связи без неправомерного технического доступа в систему. Как правило, это отказ от оплаты услуг под различными предлогами. Данный вид процветает при существовании развитой системы кредитования услуг.

В заключение отметим, что анализ криминалистической характеристики компьютерных преступлений позволяет предположить, что наибольшую значимость имеет осмотр на месте совершения компьютерного преступления:

- персональных компьютеров, серверов, устройств резервного копирования, сетевых аксессуаров;
- журналов регистрации событий защиты операционных систем и баз данных;
- документации по регламенту;
- выходной печатной документации.

Следует учитывать, что осмотр места происшествия, являясь важным источником информации, используемой для построения версий при расследовании компьютерных преступлений, не должен обладать заранее установленным приоритетом перед другими следственными действиями, так как для построения и проверки версий возможно использование фактических данных, получаемых в результате проведения иных следственных действий и оперативно-розыскных мероприятий.

2. Основные методы обеспечения компьютерной безопасности

Рассматривая особенности организации системы информационной безопасности, необходимо отметить ее многоаспектность, включающую в себя правовое, инженерно-техническое, организационное обеспечение, а также организацию управления защитой информации.

Под информационной безопасностью в общем случае понимают свойство процесса информатизации, характеризующее состояние защищенности личности, общества и государства от возможных негативных последствий информатизации.

Под безопасностью автоматизированной системы обработки информации понимают ее свойство, выражающееся в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее, то есть защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов.

Помимо мер организационно-управленческого характера, серьезную общепрофилактическую роль в борьбе с указанными преступлениями и другими правонарушениями в условиях автоматизации могут играть меры технического характера по защите машинной информации от несанкционированного доступа. При этом защита информации должна быть реализована как в правоохранительных автоматизированных системах (с особой тщательностью – в АСУ, АБД, ИПС оперативно-розыскного назначения), так и в народнохозяйственных вычислительных центрах, где необходимо предупреждать возможность внесения подлогов в информационные массивы и машинные программы обработки учетно-экономических данных.

Для организации системы защиты информации необходимо ответить на следующие вопросы: от чего, что и как надо защищать (какими методами и средствами)?

При практической отработке подходов к решению проблем безопасности информации всегда следует исходить из того, что конечной целью применения любых мер противодействия угрозам является защита владельца и (или) законных пользователей от нанесения им материального или морального вреда, а в нашем случае – и от несанкционированного доступа к государственной и служебной тайне.

Различают внешнюю и внутреннюю безопасность. Внешняя безопасность включает в себя защиту от стихийных бедствий, проникновения злоумышленников извне с целью хищения, получения доступа к носителям информации или вывода электронных систем обработки из строя. Предметом внутренней безопасности является обеспечение надежной и удобной работы электронных систем обработки, целостности программ и данных обслуживающих компьютеров.

В настоящее время существует два основных подхода к проблеме обеспечения защиты информации. Назовем их условно фрагментарный и комплексный.

Главным достоинством (и главным недостатком) фрагментарного подхода является его высокая избирательность относительно конкретной угрозы. Это обуславливает еще один основной его недостаток – локальность действия. Другими словами, эти меры обеспечивают эффективную защиту конкретных объектов от конкретной угрозы, но не более того. Даже небольшое видоизменение угрозы ведет к потере эффективности защиты.

Особенностью комплексного подхода является создание защищенной среды обработки информации, объединяющей разнородные меры противодействия угрозам (правовые, организационные, технические и др.). Этот способ реализации защиты информации определяется ее спецификой, другими объективными и субъективными факторами.

Очевидно, что реализация защищенной информационной среды позволяет гарантировать определенный уровень противодействия преступным посягательствам и оказать существенное влияние на обстановку совершения преступления.

Целостность компьютерной информации может быть нарушена и без непосредственного участия человека, что выражается:

- в повреждении или выходе из строя компьютерного оборудования в результате нестабильности системы электропитания, стихийных бедствий либо неблагоприятных условий эксплуатации;
- выходе из строя магнитных носителей информации;
- неполадках кабельных систем, вызывающих сохранение неверной информации либо снижение производительности сети;
- программных и аппаратных сбоях, возникающих в результате некорректной работы прикладного программного обеспечения либо операционных систем.

Отметим, что составными элементами системы защиты информации являются правовые (законодательные), морально-этические, административные, физические и технические (аппаратные и программные) меры.

К правовым мерам защиты относятся действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.

К морально-этическим мерам противодействия относятся всевозможные нормы поведения, которые традиционно сложились или складываются в окружающем обществе по мере развития и распространения информации. Эти нормы бывают как неписанные (например, общепризнанные нормы честности, патриотизма), так и оформленные в некий свод (устав) правил или предписаний. В частности, при обработке информации на компьютерных системах считается неэтичным производить умышленные или неумышленные действия, которые нарушают: работу компьютерных систем, целостность хранимой и обрабатываемой информации, интересы других законных пользователей, вызывают неоправданные затраты ресурсов (машинного времени, памяти, каналов связи) и т. д.

Административные меры защиты – это меры организационного характера. Они включают в себя: разработку правил обработки информации; охранные мероприятия, осуществляемые при проектировании, строительстве и оборудовании зданий (помещений), защиту от установки прослушивающей аппаратуры и т. п.; мероприятия, осуществляемые при подборе и подготовке персонала (проверка новых сотрудников, ознакомление их с порядком работы с

конфиденциальной информацией, мерами ответственности за нарушение правил ее обработки; создание условий, при которых персоналу было бы невыгодно допускать злоупотребления, и т. д.); организацию надежного пропускного режима; организацию учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией; распределение режимов доступа (профилей полномочий, паролей и т. п.); организацию подготовки и в необходимых случаях проведение скрытого контроля за работой персонала; мероприятия, осуществляемые при проектировании, разработке, ремонте и модификации оборудования и программного обеспечения компьютерных систем; сертификацию используемых технических и программных средств, строгое санкционированное рассмотрение и утверждение их изменений, проверку на удовлетворение требований защиты, документальное отражение изменений.

Физические меры защиты включают в себя разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации.

Технические (аппаратно-программные) средства защиты – электронные устройства и специальные программы для ПК, которые выполняют (самостоятельно или в комплексе с другими) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическую защиту информации и т. д.).

Таким образом, обеспечение компьютерной безопасности можно классифицировать на инженерно-техническое и организационное.

Инженерно-техническое обеспечение защиты информации – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах обеспечения безопасности учреждения.

Организационное обеспечение – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются из-за проведения организационных мероприятий.

Организационное обеспечение компьютерной безопасности включает в себя организационно-административные, организационно-технические и организационно-экономические мероприятия.

Очевидно, что в структурах с низким уровнем дисциплины и этики ставить вопрос о защите информации просто бессмысленно. В таких подразделениях надо решать прежде всего правовые и организационные вопросы.

Административные меры используются тогда, когда другие меры и средства защиты недоступны (по финансовым или техническим причинам). Однако это

не означает, что систему необходимо строить исключительно на основе административных методов, так как они имеют следующие недостатки:

- низкая надежность без соответствующей поддержки со стороны физических, технических и программных средств (люди склонны к нарушению любых установленных правил, если их можно нарушить);

- применение для защиты только административных мер обычно приводит к параличу деятельности всей организации или как минимум автоматизированной системы обработки данных (совершенно невозможно работать, не нарушая инструкций) из-за ряда дополнительных неудобств, связанных с большим объемом рутинной формальной деятельности.

Рассматривая самый распространенный и прогрессивный метод обработки информации – с помощью автоматизированных систем на базе персональных компьютеров, необходимо отметить, что проблема умышленных нарушений функционирования автоматизированных систем обработки информации различного назначения в настоящее время является одной из самых актуальных.

При использовании автоматизированных систем обработки информации можно выделить три основные причины нарушений: безответственность, самоутверждение и корыстный интерес пользователей.

Способы предотвращения этих нарушений вытекают также из природы побудительных мотивов – соответствующей подготовки пользователей, а также поддержания здорового рабочего климата в коллективе, подбора персонала, своевременного обнаружения потенциальных злоумышленников и принятия необходимых мер. Первый из них – задача руководителей органов и учреждений, второй – постоянная аналитическая работа по оценке состояния безопасности и повышению ответственности за нее всех сотрудников. Только сочетание этих способов представляет собой реальную возможность не исправлять нарушения и не расследовать преступления, а устранять их причины.

Собственно механизм реализации защиты информации подразумевает два основных способа. При первом – механизмы защиты не реализованы в программном и аппаратном обеспечении. Защита информации при хранении, обработке или передаче обеспечивается дополнительными программными или аппаратными средствами, не входящими в состав самой системы. Этот способ называется «добавленной» защитой, ибо средства защиты служат дополнением к основным программным или аппаратным средствам.

Второй способ защиты – так называемая встроенная защита. Суть ее сводится к тому, что механизмы защиты являются неотъемлемой частью автоматизированной системы обработки информации. Механизмы защиты в нем обычно реализованы в виде отдельных компонентов данной системы, распределены по другим компьютерным системам (то есть в некотором компоненте обрабатывающей системы есть часть, отвечающая за поддержание его защиты). При этом средства защиты составляют единый механизм, который

отвечает за обеспечение безопасности всей автоматизированной системы, обрабатывающей информацию. Основное достоинство этого способа – надежность и оптимальность, объясняющиеся тем, что средства защиты и механизмы их поддержки разрабатываются и реализовываются одновременно с системой обработки информации. В результате взаимосвязь средств защиты с различными компонентами системы теснее, чем при добавленной защите. Однако данная защита обладает жестко фиксированным набором функций, не позволяющим расширять или сокращать их.

Остановимся подробнее на совершенствовании системы организации защиты от утечки информации, передаваемой, обрабатываемой и принимаемой субъектами системы самыми распространенными способами: передача сообщений по телекоммуникационным системам; обработка информации с помощью ПК; обмен документами.

При осмотре приобретенных (закупленных, полученных централизованно) или возвращенных после ремонта устройств необходимо попросить поставщика (продавца, мастера по ремонту) проверить их работоспособность и принцип действия при включенных в этот момент других радиоэлектронных приборах. При наличии подозрительных сигналов на компьютерах, измерительных устройствах и других приборах зафиксировать их и четко определить, как изменились свойства устройств после их возможной доработки злоумышленником (например, из обычного сотового телефона он стал «двойником»).

Для предотвращения несанкционированного доступа к информации персонального компьютера и возможности ее похищения, модификации, копирования или изменения (порчи) необходимо рассматривать и возможность заражения программных продуктов и информационных файлов ПК компьютерными вирусами.

Компьютерный вирус – набор команд, который производит и распространяет свои копии в компьютерных системах и (или) компьютерных сетях и преднамеренно выполняет некоторые действия, нежелательные для законных пользователей информационных систем.

Таким образом, в защите информации персональных компьютеров от несанкционированного доступа можно выделить три основных направления:

- первое ориентируется на недопущение нарушителя к вычислительной среде и основывается на специальных технических средствах опознавания пользователя;
- второе связано с защитой вычислительной среды и основывается на создании специального программного обеспечения по защите информации;
- третье направление предполагает использование специальных средств защиты информации ПК от несанкционированного доступа.

Специальные технические средства опознавания пользователя персонального компьютера

Одним из способов опознавания пользователя является применение специальных электронных карточек, в которые записывается информация о владельцах, их пароли и ведется учет всех операций, выполняемых пользователем. Считывание информации производится с помощью специальных устройств-сканеров, которые могут быть ручными, тактильными или клеящимися.

Американская фирма «Software Security Inc.» разработала электронный ключ доступа к персональному компьютеру «Активатор». В ключе находится микропроцессор, в запоминающее устройство которого заносится уникальная для каждого пользователя информация. При запросе доступа к компьютеру пользователь должен поднести электронный ключ к дисплею; доступ открывается при совпадении паролей. Процедуру доступа можно модифицировать так, чтобы пароль зависел от дня недели и времени суток.

Широкое распространение получили устройства фирмы «Cal span», которые проводят идентификацию пользователей по отпечаткам пальцев. Когда палец приближается к пластине, покрытой термохромным материалом, выпуклые рубчики кожи пальца в местах соприкосновения с пластиной уменьшают температуру поверхности, изменяя при этом ее отражающую способность. Рельеф разветвлений преобразуется в цифровую форму и вводится в компьютер, где сравнивается с эталонным отпечатком данного пользователя.

Разрабатываются и применяются устройства опознавания пользователя по геометрическим признакам руки. В такой системе пользователь помещает руку на массив фотоячеек, который получает информацию о длине пальцев и их светопроводности. Затем производится сравнение полученных сигналов с эталонными, хранящимися в компьютере. Разработанные устройства не реагируют на изменение длины ногтей, но легко обнаруживают искусственные муляжи.

Достаточно надежным является способ опознавания пользователя по почерку. Для этого используются динамические характеристики процесса подписи – скорость, давление на бумагу и статические – форма и размер подписи. Подпись производится специальной ручкой, содержащей преобразователь ускорений по осям X и Y. Эти параметры определяются в процессе контрольного написания по 5–10 образцам.

Достаточно полно разработаны теоретические вопросы опознавания пользователя по голосу. На индивидуальность голоса влияют анатомические особенности и привычки человека: диапазон частот вибрации голосовых связок, высота тона; частотные характеристики голосового тракта. С точки зрения технической реализации наиболее проблемным является исследование частотных характеристик голоса. Для этого специалисты фирмы «Philips» предлагают применять специальные многоканальные фильтры с полосой

пропускания от 100 Гц до 6,2 кГц. Опознавание пользователя производится сравнением текущих данных с эталонным сигналом по каждому частотному каналу, хранящемуся в памяти ПК.

Специальное программное обеспечение по защите информации персональных компьютеров

Для защиты информации персональных компьютеров используются различные программные методы, которые значительно расширяют возможности по обеспечению безопасности хранящейся информации. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили:

- средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие до-ступ несанкционированного пользователя;
- различные методы шифрования, не зависящие от контекста информации;
- средства защиты от копирования коммерческих программных продуктов;
- защита от компьютерных вирусов и создание архивов.

Специальные средства защиты информации от несанкционированного доступа

Прохождение электрических сигналов по цепям персонального компьютера и соединительным кабелям сопровождается возникновением побочных электромагнитных излучений в окружающей среде. Распространение побочных электромагнитных излучений за пределы контролируемой территории создает предпосылки для утечки информации, так как возможен ее перехват с помощью специальных технических средств контроля. В персональном компьютере основными источниками электромагнитных излучений являются устройства ввода и вывода информации совместно с их адаптерами (монитор, принтер, клавиатура и т. д.), а также центральный процессор. Исследования показывают, что излучение видеосигнала монитора является достаточно мощным и охватывает диапазон метровых и дециметровых волн.

Для уменьшения уровня побочных электромагнитных излучений применяют специальные средства защиты информации: экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений и наводок при помощи различных резистивных и поглощающих согласованных нагрузок.

Техническому контролю в компьютерах должны подвергаться следующие потенциальные и реальные каналы утечки информации:

- побочные электромагнитные излучения в диапазоне частот от 10 Гц до 1000 МГц;
- наводки сигналов в цепях электропитания, заземления, в линиях связи;
- опасные сигналы, образующиеся за счет электроакустических преобразований, которые могут происходить в специальной аппаратуре

контроля информации. Эти сигналы должны контролироваться в диапазоне частот от 300 Гц до 3,4 кГц;

- каналы утечки информации, образующиеся в результате воздействия высокочастотных электромагнитных полей на различные провода, находящиеся в помещении, которые могут выступать в качестве приемной антенны. В этом случае проверка проводится в диапазоне частот от 20 кГц до 1000 МГц.

При контроле защиты информации персональных компьютеров используются специально разработанные тестовые программы, а также специальная аппаратура контроля уровня излучения, которые определяют режим работы компьютера, обеспечивающий совместно с другими техническими средствами скрытый режим работы для различных средств разведки.

В заключение отметим, что надежное обеспечение компьютерной безопасности будет возможно при учете проанализированных факторов и правильном решении вопросов:

Что защищать? От кого защищать? Как защищать?

ЛИТЕРАТУРА

I. Официальные документы и нормативные акты

1. Конституция Российской Федерации. – М., 1993.
2. Уголовный кодекс Российской Федерации. – М., 2002.
3. Уголовно-процессуальный кодекс Российской Федерации. – М., 2002.
4. Уголовно-исполнительный кодекс Российской Федерации. – М., 1997.
5. О милиции: Закон РСФСР от 18 апреля 1991 г. № 1026-1 (с изм. и доп. от 18 февр. и 1 июля 1993 г.) // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. – 1991. – № 16. – Ст. 503; 1993. – № 10. – Ст. 360; – № 3, 2. – Ст. 1231.
6. О правовой охране программ для электронных вычислительных машин и баз данных: Закон Российской Федерации от 23 сентября 1992 г. № 3523-1 // Ведомости Съезда народных депутатов и Верховного Совета РФ. – 1992. – № 42. – Ст. 2325.
7. О государственной тайне: Закон Российской Федерации от 21 июля 1993 г. № 5485-1 // Рос. газ. – 1993. – 21 сент.
8. Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы: Закон Российской Федерации от 21 июля 1993 г. № 5473-1 // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. – 1993. – № 33. – Ст. 1316.
9. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г.
10. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г

11. О безопасности: Закон Российской Федерации от 5 марта 1992 г. № 2446-1 // Ведомости Совета народных депутатов и Верховного Совета РФ. – 1992. – № 15. – Ст. 769.

12. О связи: Федеральный закон от 7 июля 2003 г. № 15-ФЗ // Рос. газ. – 2003. – 14 июля.

13. Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств: Указ Президента Российской Федерации от 30 ноября 1995 г. № 891 // Собрание законодательства РФ. – 1999. – № 24. – Ст. 2954.

14. О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации: Указ Президента Российской Федерации от 9 января 1996 г. № 21 // Собрание законодательства РФ. – 1996. – № 3. – Ст. 153.

15. Об утверждении перечня сведений конфиденциального характера: Указ Президента Российской Федерации от 6 марта 1997 г. № 188 // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

16. О перечне сведений, отнесенных к государственной тайне: Указ Президента Российской Федерации от 24 января 1998 г. № 61 // Собрание законодательства РФ. – 1998. – № 5. – Ст. 561.

17. Доктрина информационной безопасности Российской Федерации: Утв. Указом Президента Российской Федерации от 9 сентября 2000 г. № Пр–1895 // Рос. газ. – 2000. – 28 сент.

18. Комментарий к Уголовно-исполнительному кодексу Российской Федерации / Под ред. А.И. Зубкова. – М.: ИНФРА-М – НОРМА, 1997.

19. Комментарий к Федеральному закону «Об оперативно-розыскной деятельности». – М., 1997.

20. Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности: Постановление Правительства Российской Федерации от 1 июля 1996 г. № 770 // Собрание законодательства РФ. – 1996. – № 28. – Ст. 3382.

21. Федеральная программа по усилению борьбы с преступностью: Постановление Правительства Российской Федерации от 10 марта 1999 г. № 270 // Собрание законодательства РФ. – 1999. – № 12. – Ст. 1484.

22. Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию: Постановление Правительства Российской Федерации от 10 марта 2000 г. № 214 // Собрание законодательства РФ. – 2000. – № 2. – Ст. 1215.

23. Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд: Утв. приказом ФСНП РФ, ФСБ РФ, МВД РФ, ФСО РФ, ФПС РФ, ГТК РФ, СВР РФ от 13.05.1998г. № 175/ 226/ 336/ 201/ 286/ 410/56.

II. Учебники, монографии, пособия

24. *Андрианов В.И., Соколов А.В.* Устройства для защиты объектов и информации: Справ. пособие. - М.: АСТ; СПб:Полигон, 2000.

25. *Андрианов В.И., Бородин В.А., Соколов А.В.* «Шпионские штучки» и устройства для защиты объектов и информации: Справ. пособие. - СПб: Лань, 1996.

26. *Барабанов Н.П., Кленов С.Н.* Обеспечение безопасности информации в уголовно-исполнительной системе. – Рязань: Академия права и управления Минюста России, 2003.

27. *Бородин В.И., Шайтанов А.В.* Оперативно-техническое обеспечение раскрытия преступлений органами внутренних дел: Лекция. – М.: Юрид. ин-т МВД РФ, 1994.

28. *Волчков И.М.* Оперативно-розыскная информация: сущность и методология ее реализации: Учеб.пособие. – Псков, 2002.

29. Влияние научно-технического прогресса на юридическую жизнь / Под ред. Ю.М.Батурина. - М.: Юрид. лит., 1988.

30. *Генин О.И., Епифанов С.С., Кленов С.Н.* Организация связи и автоматизированного управления // Организация управления в уголовно-исполнительной системе: Учебник. Т.1, Гл. 17. - Рязань: Академия права и управления Минюста России, 2002.

31. *Демидов В.А., Сильников М.В., Шайтанов А.В.* Техника связи ОВД: Учеб. пособ. / Под ред. В.П.Сальникова. - СПб, 2000.

32. *Ильин А.Н.* Основы специальной техники ОВД: Учеб. пособие. – М.: ГУК МВД РФ, 1997.

33. *Кленов С.Н.* Защита информации от прослушивания: Учеб.- метод. пособие - Рязань: Академия права и управления Минюста России, 2001.

34. *Наумкин Ю.В.* Научно-технический прогресс и проблемы борьбы с преступностью: Учеб. пособие. - М., 1990.
35. Основы информационной безопасности: Учебник. – Воронеж, 2001.
36. *Рудометов Е.А., Рудометов В.Е.* Электронные средства коммерческой разведки и защиты информации: Справ. пособие. – СПб.: Полигон, М.: АСТ, 2000.
37. *Рудометов Е.А., Рудометов В.Е.* Электронные устройства двойного применения. – СПб.: Полигон, М.: АСТ, 2000.
38. Научно-технический прогресс: Словарь. - М.,1987.
39. *Соколов А.В., Степанюк О.М.* Методы информационной защиты объектов и компьютерных сетей - М.: АСТ; СПб: Полигон, 2000.
40. Специальная техника и информационная безопасность: Учебник / Под ред. В.И.Кирина. Т.1., М.: Академия управления МВД РФ, 2000.
41. Технические методы и средства защиты информации / Ю.Н.Максимов, В.Г.Сонников, В.Г.Петров и др. - СПб.: Полигон, 2000.
42. *Овчинский С.С.* Оперативно-розыскная информация. / Под ред. А.С.Овчинского и В.С.Овчинского. М.: ИНФРА – М, 2000.
43. Оперативно-розыскная деятельность: Учебник / Под ред. К.К.Горяинова, В.С.Овчинского, Г.К.Синилова, А.Ю.Шумилова. – М.: ИНФРА-М, 2004.
44. Организация охраны и совершенствование оборудования объектов УИС инженерно-техническими средствами охраны и надзора: Сб. материалов положит. опыта. М.: НИИ ФСИН России, 2005.
45. *Хогг Я.* Средства для борьбы с терроризмом. – М.: ЭКСМО-Пресс, 2001.