Министерство внутренних дел
Российской Федерации

Краснодарский университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ, ТЕРРОРИЗМУ И ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ

Материалы
межвузовской научно-практической
конференции, посвященной Дню российской науки

(10 февраля 2014 г.)

Краснодар
КрУ МВД России
2015

УДК 343
ББК 67.410
И74

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Информационная безопасность и противодействие
И74 угрозам экстремизму, терроризму и организованной преступности : материалы межвузовской научно-практической конференции, посвященной Дню российской науки, 10 февраля 2014 г. / редкол.: А. Б. Сизоненко, С. Г. Клюев, А. Г. Александров, В. Н. Цимбал, М. Н. Андрющенко. – Краснодар : Краснодарский университет МВД России, 2015. – 226 с.

ISBN 978-5-9266-0853-0

Представлены доклады и тезисы выступлений участников межвузовской научно-практической конференции, посвященной Дню российской науки, в которых рассматриваются проблемы информационной безопасности и борьбы с терроризмом, экстремизмом и организованной преступностью.

Для преподавателей, аспирантов и слушателей образовательных учреждений МВД России, а также практических сотрудников органов внутренних дел.

УДК 343
ББК 67.410

ISBN 978-5-9266-0853-0

Алифанова А.В.,
курсант 2 курса
Краснодарского университета МВД России;
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Роль противодействия угрозам информационных войн в системе обеспечения информационной безопасности

В настоящее время тема информационной войны имеет большую актуальность. Ее сущность раскрывается в притче «Черепаха и информационные технологии»1, где С.П. Расторгуев говорит о том, как лиса путем информационного воздействия, а именно распространением слухов, размещением плакатов о летающих черепахах, заставила своего противника поверить в новую жизнь и добровольно вылезти из панциря. Теперь черепаха никогда не узнает, что информационная война – это целенаправленное обучение врага тому, как снимать панцирь с самого себя.

Первоначально термин «информационная война» использовал Томас Рона в 1976 году. Активно употребляться в прессе этот термин стал после проведения операции «Буря в пустыне» в 1991 г., где новые информационные технологии впервые были использованы как средства ведения боевых действий.

Информационная война – воздействия на гражданское население и военнослужащих другого государства, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, процессам ее получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования, а также совокупности технического, программного и организационного обеспечения противника при одновременной защите собственной информации, информационных процессов и информационных систем.

[1]С.П. Растогуев Формула информационной войны. Серия «Национальная безопасность». Выпуск 1. - М.: Белые Альвы, 2005. - 96 с.

Информационная безопасность – это состояние информационной среды обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации, то есть состояние информации, при которой обеспечена ее конфиденциальность, целостность и доступность; а также защиту субъектов от негативного воздействия.

Информационные войны могут вестись:

– между государствами;

– между властью и оппозицией;

– между финансово-промышленными группами.

Наиболее известным примером информационной войны между государствами является холодная война между СССР и США, которая длилась с 1946 по 1991 год, где применение западными государствами средств и методов информационного воздействия на население Советского Союза привело, на ряду с другими причинами, к распаду СССР.

В Украине произошел кризис власти и в настоящее время ведется гражданская война. Она характеризуется рядом острых конфликтов в борьбе за изменение национально-государственного устройства между различными политическими, национальными и социальными группами на территории современной Украины. Одним из основных методов ведения этой войны является именно информационное противоборство. Этот пример раскрывает сущность войны между властью и оппозицией.

Информационная война между финансово-промышленными группами выражается в совершении промышленного шпионажа и хищении оригинальных решений. Имеет место информационное давление на потребителей и применение компромата относительно отдельных производителей.

Сегодня в постиндустриальном, информационном обществе, все меньше используется «физическое оружие» и все чаще главенство берет оружие информационное. Не обязательно завоевывать страны физически, достаточно завоевать идеологически, так как в современных условиях информационная индустрия является одним из главных источников развития общества. Отставание в этой сфере, напротив, равносильно потере статуса мировой державы. Целенаправленное изменение жизненных стиля, принципов, стандартов и моделей потребления и поведения населе-

ния, особенно молодежи, с помощью информационных технологий направлено на стратегическое использование информации, подрыв государства изнутри, что не всегда и не сразу воспринимается как информационная агрессия, – именно этим она опаснее для страны, против которой направлена. Информационная война в настоящее время идет на полосах газет, в эфире радио и телевидения, на сайтах и порталах Интернета.

Злоупотребление свободой массовой информации является одним из главных внутренних источников угроз информационной безопасности России. Около 40% разведывательной информации получается в процессе аналитической обработки открытых материалов, включая печатные и электронные СМИ.[1] Политическая, экономическая, социальная, культурная системы России находятся в стадии модернизации, что еще в большей степени актуализирует проблемы обеспечения безопасности страны, в том числе и информационной.

Государственными органами РФ, контролирующими деятельность в области защиты информации являются:

– комитет государственной думы по безопасности;

– совет безопасности России;

– федеральная служба по техническому и экспортному контролю (ФСТЭК);

– федеральная служба безопасности России (ФСБ России);

– министерство внутренних дел Российской Федерации (МВД России).

Государственная политика в Российской Федерации по обеспечению информационной безопасности реализуется через правотворчество, правоприменение и участие государства в развитии правосознания и правовой культуры граждан. Важность проблемы информационной безопасности подтверждается принятием Доктрины информационной безопасности Российской Федерации, которая раскрывает цели, задачи, принципы и основные направления обеспечения информационной безопасности России.

Современные информационные войны крайне опасны, так как нацелены на подрыв политических, экономических и соци-

[1] Информационная безопасность: учеб. пособие /С.В. Петров, И.П. Слинькова, В.В. Гафнер, П.А. Кисляков. - Новосибирск: АРТА, 2012 - 296 с. - (Серия «безопасность жизнедеятелбности».

альных основ государств-противников, их территориальное раздробление, обеспечение благоприятных материальных и экологических условий жизни своего населения за счет других государств. В этих условиях необходим правильный выбор защиты информационных акций, верная расстановка сил и средств, что невозможно без глубокого научного осмысления современных реалий информационного противоборства. Для противостояния угрозам в информационной сфере и использования относительного преимущества над некоторыми из потенциальных противников необходима четкая концепция информационной безопасности и долгосрочная государственная политика по созданию ее материальной базы.

Афанасьев В.В.,
слушатель 5 курса
Краснодарского университета МВД России;
научный руководитель:
Стукалов В.В.,
доцент кафедры ОРД в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

История развития экстремизма в России

В современной России экстремизм и его крайнее выражение – терроризм стали едва ли не главной угрозой человеку и обществу. Между тем, экстремизм отнюдь не новое явление в истории России. 4 апреля 1866 г. выстрел полубезумного Каракозова возвестил о начале эпохи экстремизма в России. С тех пор он стал средством решения практически всех конфликтов и проблем, возникающих в обществе и государстве. Более того, самым простым, не требующим ни особых интеллектуальных усилий, ни экономических затрат, ни дипломатического искусства. Экстремизм как терроризм предполагал полное неуважение к человеческой жизни, отрицание какой-либо ее ценности.

К экстремистским и собственно террористическим действиям прибегали народовольцы, эсеры, большевики, другие политические группы, охваченные ненавистью и фанатизмом. Сам коммунистический режим был экстремистским, особенно в эпоху правления Ленина и Сталина. Поэтому следует честно признать, что в нынешней России экстремизм, закрепившись в общественных нравах и став частью идеологии и психологии некоторых социальных групп, лишь продолжил свою прежнюю жизнь, приняв новые, подчас более изощренные и угрожающие формы. Принципиальным здесь является то, что сейчас он идет не от государства «вниз», а «снизу» к нему и к людям. Вот почему так важно знать причины названного явления, что позволяет определить главные объекты профилактических и предупредительных мер со стороны власти и населения.

В некоторых публикациях, даже научных, приходится встречать утверждение, что экстремизм в нашей стране получил широкое распространение потому, что в ней живет много наций и бытует множество разных религий. Но это поверхностное и ложное суждение, могущее увести от установления подлинных причин экстремизма и тем самым косвенно способствовать ему, ослабить защиту личности и общества от экстремистского насилия[1].

До революции Россия была в основном крестьянской страной со слабыми миграционными потоками; города, в которых все могли перемешаться, росли медленно. И, как утверждают специалисты, урбанизация в стране не совершила своего полного цикла до сих пор. До революции промышленность только начала развиваться, и хотя темпы ее роста были высокими, процесс индустриализации был прерван октябрьской революцией и отброшен назад гражданской войной. Бизнес исчез, предпринимательская деятельность преследовалась в уголовном порядке вплоть до последних дней советской власти. Люди работали за копейки, их трудовой энтузиазм исчезал по мере того, как ослабевала вера в достижимость «светлого будущего» коммунизма.

В СССР люди, несмотря на демагогию о социалистическом интернационализме и дружбе народов, фактически оказались разделены еще и административно-территориально. «Мудрые»

[1] http://razumru.ru/humanism/journal/56/antonyan.htm

вожди закрепили и рассортировали этносы. «Очень хорошие» получили статус союзных республик, «просто хорошие» – автономных, а далее следовали автономные округа и т.п. Это породило зависть и националистические разграничения людей разных этносов между собой, однако, верховная государственная власть старалась маскировать неравноправие пропагандой идей культурного богатства и самобытности «больших» и «малых» народов СССР. Но как только она ослабла, и обнажилось реальное положение вещей, ненависть и вражда между людьми разных национальностей буквально захлестнули отдельные районы СССР (например, в Средней Азии), а после его распада – некоторые бывшие союзные республики (например, в Грузии).

С распадом СССР и по настоящее время труд не стал полем сплочения людей, его оплата не возросла, а малый и средний бизнес, несмотря на все призывы и усилия руководства страны, не стал локомотивом экономики. Подавляющее большинство населения имеет низкий материальный достаток. В целом – это благодатная почва для возникновения и распространения экстремистских и даже фашистских настроений.

Когда люди бедствуют, они очень тревожны и ищут причины своего неблагополучия, ищут виновников. Здесь самое простое – обвинить тех, кто говорит на другом языке или молится другому богу, или не так выглядит. Потому что истинных виновников им найти трудно. Прежде всего в силу низкого культурного уровня и забитости нуждой. А эти другие – рядом, особенно если это меньшинство или это группы незащищенного населения, их можно легко унизить, совершить над ними насилие и даже уничтожить.

Здесь «героем» становится человек толпы – примитивный и злобный, наделенный способностью лишь черно-белого видения мира. Ему нужны «простые» решения, и он готов сорваться в любой момент; такие люди есть во всех странах. Особую ненависть у человека экстремистского сознания вызывают «неграждане» России. Они – чужие, виновники «наших» бед или, в конце концов, козлы отпущения, на которых можно вылить свою злобу.

Говоря о вопросах национального и общегражданского единства в связи с противодействием экстремизму, нельзя не сказать об особой роли Русской православной церкви (РПЦ). Эта

церковь всегда призывала к тому, чтобы люди довольствовались малым и не стремились к значительным экономическим успехам, одним словом, чтобы жили в пределах самого необходимого. Но аскетизм несовместим с материальным достатком, которого можно добиться только в упорном труде. Такая психология и идеология во многом проложила дорогу большевизму, который тоже призывал к бедности и воздержанию ради светлейшего будущего – коммунизма. На идею коммунистической утопии были перенесены многие упования православной веры: всеобщее изобилие, мир, блаженство и счастье всего человечества – чем не земной аналог царствия небесного? Большевикам не нужно было «переделывать» народ, нужно было использовать ментальность населения, только наполнив ее другими словами. Но главное – он был беден, был убежден и его продолжали убеждать в праведности бедности. Таким образом, и церковная, и большевистская веры задерживали развитие народа, не освобождали его сознание, не позволяли посмотреть на мир открыто и широко. Исторически замороженные этносы и народности продолжали быть разобщенными, хотя по многим внешним параметрам они давно жили на одной территории под одной властью. Под внешним единством глубоко лежали семена экстремизма.

Делая акцент на значении свободного труда и материального благополучия, мы не затрагиваем проблему, для чего человеку материальные возможности. Очевидно, что любому нормальному человеку и здоровой семье они нужны для создания благоприятных условий жизни, для образования и интеллектуального роста, духовного обогащения, помощи другим и т.д. Но чтобы достичь этого, надо упорно трудиться, а в труде, адекватно оплачиваемом, люди лучше понимают друг друга, уважают друг друга, они становятся равноправными и, следовательно, сплоченными в своих правах и обязанностях.

В наши дни РПЦ, к сожалению, не изменила свою позицию по отношению к материальному благосостоянию людей. Совсем недавно глава РПЦ призвал не стремиться к экономической выгоде, что прямо противоречит установкам руководства страны. Невозможно представить себе бизнесмена, даже самого маленького, который не стремился бы к экономической выгоде. В про-

тивном случае его бизнес немедленно рухнет. В этой связи стоит напомнить, что наиболее значительный, даже бурный промышленный рост был в тех западных странах, в которых протестантская церковь прямо и недвусмысленно призывала к обогащению. Но нельзя сказать, что в таких странах (Великобритания, Германия, Нидерланды, США) все люди увязли в грехах, не думали и не думают о спасении души, у них получается и то, и другое – и активный труд, в том числе и в сфере предпринимательства, и горячие молитвы, соблюдение религиозных обрядов и ритуалов[1].

К сожалению, и сегодня для многих россиян безразличие к материальной стороне жизни и отсутствие экономического сознания обернулись пьянством, а то и наркоманией. Необходимо отметить, что пьянство и алкоголизм в основном порождаются неумением и нежеланием работать, отсутствием стремления к экономической выгоде, а отсюда – ощущение обреченности и безысходности, выброшенности и ненужности, бедность, озлобление на весь мир.

Общая неудовлетворенность и попытки преодолеть ее незаконными способами порождаются и невозможностью удовлетворить жизненно важные потребности, и ощущением несправедливости, неравенства по сравнению с другими социальными группами. Преимущества последних в доступности материальных и духовных благ, даже если они являются результатом упорного и добросовестного труда, воспринимаются обездоленными слоями населения как приобретенные за их счет или путем обмана. По большей части здесь имеет место бессознательный перенос некоторых своих недостатков на других и отношение к ним уже как к носителям таких недостатков. Однако ненависть к другим практически никогда не приводит к повышению материального благосостояния и расширению социальных возможностей бедных слоев населения, по существу исключенных из общества и оказавшихся на обочине экономического и социального развития.

[1]Витюк В.В, Эфиров С. А. «Левый» терроризм на Западе: история и современность / В. В. Витюк, С. А. Эфиров ; Отв. ред. Г. В. Осипов; АН СССР, Ин-т социол. исслед., М. Наука 1987 с .315

К исторически обусловленным экстремогенным факторам следует отнести некоторые особенности политической психологии народов России:

1. Приверженность монархической идее, которая берет свое начало в глубокой древности и нашла воплощение в российской абсолютной монархии, причем уже в те периоды истории, когда от нее стали постепенно отказываться западные страны. Принцип идеологического и классового абсолютизма мощно расцвел в коммунистической диктатуре, но не исчез и после ее распада. И сейчас сохраняется упорная вера во всесилие «элит», в полезность и целесообразность сильной, даже очень сильной и никому не подотчетной руки. Общественная опасность монархической идеи в нынешних условиях состоит в заключенной в ней норме решать проблемы с позиции силы и не вступать в диалог с оппонентами.

2. Близкая к паранойе установка, что кругом сплошные враги и все наши беды от них, внутренних и внешних. Особенно преуспели в этом большевики. Число врагов у них было неисчерпаемо много: от царей до членов политбюро. Их нужно было ненавидеть, выявлять, преследовать, уничтожать. Архетип чужого, врага в коммунистические годы можно отнести к самым распространенным, и живучим. Он не исчез, проявляясь сейчас, например, в активном антизападничестве, стигматизации отдельных национальных, религиозных и иных социальных групп. Отнюдь не изжит антисемитизм, усилилось презрительное и даже враждебное отношение к представителям народов Кавказа и Средней Азии.

3. Исконное недоверие в России к демократии, в силу невежества и отсутствия демократического опыта жизни, порождает подозрительность, ее отождествление с хаосом и разрушением, в лучшем случае с тем, что ни в коем случае не обеспечит безопасность и благополучие.

Все названные явления социальной жизни тесно взаимосвязаны и изолировано существовать не могут. Это придает им повышенную общественную опасность.

Белоусов В.О.,
слушатель 5 курса
Краснодарского университета МВД России
Научный руководитель:
Сафронов А.А.,
доцент кафедры ОРД в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент

Роль международных организаций в антитеррористической деятельности

Говоря о международном сотрудничестве в области борьбы с терроризмом, линию рассуждений необходимо начинать с Организации Объединенных Наций, как центра сосредоточения сил и воль её участников.

Декларация и Программа действий, принятая на Всемирной конференции ООН по правам человека 25 июня 1993 г. в Вене, определила, что акты, методы и практика терроризма во всех его формах и проявлениях являются деятельностью, которая направлена на уничтожение прав, основных свобод и демократии, создает угрозу территориальной целостности и безопасности государств и дестабилизирует законные правительства. В продолжение данных тезисов на 49-й сессии Генеральной Ассамблеи Организации Объединенных Наций (1994) принята Декларация о мерах по ликвидации международного терроризма, в которой выражается убежденность в целесообразности более тесной координации и сотрудничества между государствами в борьбе с преступлениями, связанными с терроризмом, включая оборот наркотиков, незаконную торговлю оружием, «отмывание денег» и контрабанду ядерных и других потенциально смертоносных материалов. В этом контексте государствам предлагается в срочном порядке провести обзор сферы применения существующих международно-правовых положений о предупреждении, пресечении и ликвидации терроризма во всех его формах и проявлениях с целью обеспечить наличие всеобъемлющих правовых рамок, включая все аспекты этого вопроса.

В свою очередь, на совещании по борьбе с терроризмом (Париж, 30 июля 1996 г.) министры стран «большой восьмерки» приняли итоговый документ, в котором заявили о своей решимости уделять первостепенное внимание борьбе с терроризмом, сделали обзор новых тенденций развития терроризма в мире. Участники форума представили на итоговой пресс-конференции согласованный ими список из 25 мер по борьбе с терроризмом, значительная часть которых касается национальной компетенции государств. Одна из рекомендаций относится к «улучшению взаимодействия между отдельными органами и ведомствами, которые занимаются различными аспектами данной проблемы». Речь идет также об улучшении подготовки квалифицированных специалистов по антитеррористическим действиям, в том числе для «предотвращения терроризма с использованием радиоактивных, химических, биологических и отравляющих веществ».

В отдельный пункт выделено принятие национальных законов с целью более эффективного контроля за производством, торговлей и экспортом оружия и взрывчатки.

Документ обязывает подписавшие его страны отказаться от любой пассивной или активной поддержки террористов; ужесточить юридические меры преследования за террористическую деятельность; отдавать под суд любое лицо, обвиняемое в совершении, подготовке террористических актов или оказании помощи в их осуществлении.

«Восьмерка» рекомендовала всем государствам препятствовать передвижениям групп террористов и их отдельных членов и в этих целях ввести более строгий пограничный контроль и правила оформления удостоверений личности и визовой документации.

Организация Объединенных Наций осуществляет программы борьбы с терроризмом в рамках своих департаментов, подразделений и учреждений, включая:

Контртеррористический комитет (КТК), который контролирует осуществление резолюции 1373 (2001) и представляет доклады Совету Безопасности;

Совет Безопасности, который занимается вопросом терроризма как угрозы международному миру и безопасности. Он встречается для рассмотрения структуры и деятельности КТК на

регулярной основе и при необходимости обсуждает более широкие вопросы, связанные с терроризмом;

Рабочую группу Организации Объединенных Наций по разработке политики в отношении терроризма, которая была учреждена Генеральным секретарем в октябре 2001 года и уполномочена изучать последствия и широкие аспекты политики борьбы с терроризмом применительно к Организации Объединенных Наций и сформулировать рекомендации. Рабочая группа по разработке политики определила порядок интеграции деятельности Организации Объединенных Наций в рамках трехсторонней стратегии в поддержку глобальных усилий, чтобы не допустить вовлечения в терроризм недовольных групп населения, закрыть доступ группам или отдельным лицам к средствам совершения актов терроризма и поддерживать широкое сотрудничество в борьбе против терроризма.

Резолюция Совета безопасности ООН от 28 сентября 2001 года № 1373, устанавливая определенные обязанности для государств, призывая к действиям во исполнение указанных в ней обязанностей, постановляет «учредить, в соответствии с правилом 28 своих правил процедуры, комитет Совета Безопасности, состоящий из всех членов Совета, для контроля за осуществлением настоящей резолюции, с использованием необходимых экспертов».

Структура органа представляет собой следующую систему. Комитет Совета Безопасности состоит из 15 членов Совета Безопасности. Во исполнение резолюции 1373 (2001) от 28 сентября 2001 года были избраны Председатель и заместители Председателя Комитета. В рамках органа учреждены подкомитеты: A, B и C. Все члены распределены по указанным подкомитетам следующим образом:

A: Бразилия, Дания, Российская Федерация, Филиппины, Франция;

B: Греция, Китай, Румыния, Соединенные Штаты Америки, Танзания;

C: Алжир, Аргентина, Бенин, Соединенное королевство Великобритании и Ирландии, Япония.

В резолюции 1535 (2004) от 26 марта 2004 года Совет Безопасности одобрил доклад Контртеррористического комитета (КТК) об активизации его работы (S/2004/124) и учредил Испол-

нительный директорат Контртеррористического комитета (ИДКТК), с тем чтобы усилить способность Комитета контролировать осуществление резолюции 1373 (2001) и эффективно продолжать работу по наращиванию потенциала, которой он занимается.

Необходимость активизации работы КТК, о которой говорится в вышеупомянутом докладе, особенно актуальна, поскольку КТК стал играть более инициативную роль в таких областях, как диалог с государствами-членами, оценка хода выполнения резолюции 1373 (2001), содействие оказанию технической помощи государствам-членам и поощрение более тесного сотрудничества и координации с международными, региональными и субрегиональными организациями.

КТК является вспомогательным органом Совета Безопасности. Он регулярно отчитывается перед Советом о своей деятельности как в письмах Председателя на имя Председателя Совета Безопасности, так и в устных докладах на заседаниях Совета Безопасности, посвященных терроризму.

Совет Безопасности направляет и контролирует работу КТК. Он регулярно рассматривает структуру и деятельность КТК. Совет просит КТК представлять его «программу работы» для сведения своих членов. Председатель КТК уведомляет Председателя Совета Безопасности о получении Комитетом доклада от государства-члена и о сроках отправки ответа КТК на этот доклад.

Резолюция 1373 (2001) имеет широкую сферу охвата, включающую национальное законодательство, внутренние исполнительные механизмы и международное сотрудничество. Для того чтобы государства могли сосредоточить свое внимание на принятии эффективных мер в областях, имеющих для них приоритетное значение, КТК определил для своей работы с государствами три этапа анализа:

Этап А) В первую очередь КТК устанавливает, имеется ли у государства эффективное законодательство по борьбе с терроризмом во всех областях деятельности, связанной с резолюцией 1373 (2001), уделяя особое внимание борьбе с финансированием терроризма.

КТК придает этому законодательству особое значение, поскольку без эффективной законодательной основы государства не

могут создать исполнительный механизм предотвращения и пресечения терроризма и привлечения к судебной ответственности террористов и тех, кто оказывает им поддержку. Борьба с финансированием терроризма включена в Этап А в качестве одной из первоочередных задач, поскольку в пункте 1 постановляющей части резолюции 1373 (2001) этому аспекту борьбы с терроризмом уделяется особое внимание.

В целях обеспечения методического и последовательного подхода при рассмотрении третьих и последующих докладов государств особое внимание будет по-прежнему уделяться Этапу А до тех пор, пока у КТК не будет никаких дальнейших замечаний по этому этапу.

Этап В) После того как государства примут законодательство, охватывающее все аспекты резолюции 1373, можно будет перейти к следующему этапу. На этом этапе государство должно быть в полной мере готово к осуществлению резолюции 1373 (2001) в соответствии с его обязанностями и в рамках его суверенной юрисдикции, при этом оно должно укреплять его исполнительный механизм для обеспечения соблюдения его законодательства, связанного с резолюцией 1373 (2001).

С учетом накопленного опыта этап В может включать вместе с эффективным и скоординированным исполнительным механизмом деятельность, охватывающую все аспекты резолюции 1373 (2001) и, в частности, предотвращение вербовки членов террористических групп, передвижения террористов, предоставления им убежища и оказания любых других форм активной и пассивной поддержки террористам или террористическим группам.

Эффективный исполнительный механизм включает, в частности, следующее:

правоохранительные и разведывательные органы и для выявления, наблюдения и задержания тех, кто занимается террористической деятельностью, и тех, кто оказывает ей поддержку;

службы таможенного, иммиграционного и пограничного контроля для предотвращения передвижения террористов и предоставления им убежища;

механизмы предотвращения доступа террористов к оружию.

Этап С) С учетом того, что в разных странах эта деятельность осуществляется в разных условиях, прогресс в деле реше-

ния этих первоочередных задач будет неоднозначным. КТК признает, что меры, принимаемые государствами, следует рассматривать на индивидуальной основе, однако он призывает все государства добиваться осуществления резолюции 1373 (2001) по возможности самыми быстрыми темпами.

Что касается дальнейших перспектив, то на каком-то этапе КТК необходимо будет рассмотреть вопрос о его диалоге с государствами, в которых уже имеется надлежащее законодательство, охватывающее все аспекты резолюции 1373 (2001), и надлежащие исполнительные механизмы для осуществления этого законодательства и которые уже не входят в число тех государств, которые требуют первоочередного внимания. В таких случаях КТК, возможно, перейдет к обеспечению контроля за Этапом С осуществления резолюции 1373 (2001), используя результаты, достигнутые на этапах А и В и охватывая оставшиеся области резолюции 1373 (2001).

Белоусова Н.В.,
курсант 1 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Средства локализации взрыва

Террористические акты на сегодняшний день стали не просто редкими статьями на полосах газет или страницах блогов в Интернете, а обыденностью повседневной жизни.

В соответствии с российским законодательством, а именно в п. 1 ст. 3 ФЗ «О противодействии терроризму» от 06.03.2006 № 35-ФЗ под терроризмом понимается: «Идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения

и (или) иными формами противоправных насильственных действий».

Правовую основу противодействия терроризму составляет Конституция Российской Федерации, общепринятые принципы и норма международного права, международные договоры Российской Федерации, указанный выше ФЗ от 06.03.2006 № 35-ФЗ и иные федеральные законы, нормативно-правовые акты Президента Российской Федерации, нормативно-правовые акты Правительства Российской Федерации, а также принимаемые в соответствии с ними нормативные правовые акты других федеральных органов государственной власти.

Основной формой пресечения террористического акта является контртеррористическая операция, которая предусматривает «Реализацию комплекса специальных, оперативно-боевых, войсковых и иных мероприятий с применением боевой техники, оружия и специальных средств по пресечению террористического акта, обезвреживанию террористов, обеспечению безопасности граждан, организаций и учреждений, а также по минимизации и (или) ликвидации последствий проявлений терроризма»[1].

Если рассмотреть статистику совершения террористических актов, то в докладе Национального консорциума по изучению терроризма и ответов на терроризм при Мэрилендском университете США отмечается, что в 2012 году 8500 террористических актов по всему миру унесли жизни почти 15,5 тыс. человек. 2012 год – рекордный по числу терактов и количеству жертв. Наблюдения ведутся с 1970 года. Исследователи отмечают, что большая часть терактов совершалась в тех странах, где доминирует мусульманское население[2].

К антитеррористическим средствам и системам относятся следующие группы поисковых устройств:

- средства визуального контроля;
- металлоискатели;
- рентгено-просмотровая техника;
- газоанализаторы;

---

[1]См.: ст. 23 Концепции противодействия терроризму в Российской Федерации (утв. Президентом РФ от 05.10.2009).

[2]Википедия. Свободная энциклопедия. URL: http:\\ru.wikipedia.org/wiki / Терроризм (дата обращения: 07.01.2014).

– обнаружители оптических устройств;
– детекторы состава веществ, основанные на ядерно-физических методах (нейтронный, фотоядерный, ядерно-магнитного и ядерно-квадрупольного резонансов и др.);
– нелинейные радиолокаторы;
– обнаружители приемников радиоуправляемых взрывных устройств;
– обнаружители временных замедлителей взрывных устройств;
– беспилотные летательные аппараты.

К средствам нейтрализации террористических угроз можно отнести следующие технические устройства:

– роботизированная техника;
– постановщики радиопомех, используемые при работе с подозрительными предметами;
– разрушители подозрительных предметов;
– локализаторы подозрительных предметов;
– взрывозащитные средства.

Террористические взрывы в местах массового скопления людей являются наиболее опасными. Одна только угроза взрыва, возникающая при обнаружении подозрительного предмета, влечет за собой приостановку работы объекта и эвакуацию людей. С момента обнаружения взрывного устройства (далее - ВУ) и до приезда специалистов-взрывотехников персонал оказывается лицом к лицу с угрозой разрушительного взрыва.

После обнаружения ВУ или взрывоопасного предмета необходимо принять контрмеры по предотвращению возможных последствий взрыва или максимальному ослаблению его действий. Прежде всего, следует осуществить эвакуацию людей и изоляцию опасной зоны, а также экстренным образом вызвать специалистов по взрывотехнике.

В основном средства локализации взрыва подразделяются на: противоосколочные одеяла, взрывозащитные контейнеры и эластичные контейнеры.

Противоосколочные одеяла бывают как легкие, так и тяжелые. Предназначаются они для локализации поражающих факто-

ров взрыва как осколочных, так и фугасных боеприпасов различных типов.

Конструктивно «одеяло» представляет собой защитный пакет, выполненный из высокомодульных тканей (СВМ, таврон, кевлар) и баллистического нейлона.

К недостаткам изделий подобного типа можно отнести, неудобство укладки на взрывоопасные предметы, расположенные вблизи вертикальных стенок, под скамейками, в углах помещения и т.п. Кроме того, существенным недостатком является возможность приведения к срабатыванию взрывателей с магнитным датчиком цели при укладке одеяла на взрывоопасные предметы, а также исключение возможности обезвреживания взрывоопасных предметов с помощью разрушителей ближнего радиуса действия или огнестрельного оружия. Необходимо учитывать, что при взрыве под одеялом осколочных боеприпасов, например, ручных гранат, имеется значительная вероятность «выдувания» и разлета в приземном слое воздуха некоторой части осколков.

Для безопасного хранения и транспортировки ВУ и взрывных веществ (далее – ВВ) взрывотехническими службами используются взрывозащитные контейнеры. По своей конструкции взрывозащитные контейнеры разделяются на два типа: закрытые и полуоткрытые.

Контейнеры закрытого типа обеспечивают полную защиту окружающего пространства от воздействия ударной волны, осколков и других поражающих факторов взрыва и предназначены для эвакуации и хранения ВУ, токсичных и радиационных материалов.

Контейнеры полуоткрытого типа являются средством оперативной защиты от взрывоопасных предметов. Чаще всего представляют собой, урну с открытым верхом и предназначены для размещения в местах массового скопления людей. Данная конструкция обеспечивает локализацию поражающего действия осколочных и безоболочковых взрывоопасных предметов с массой заряда ВВ до 1,0 кг в тротиловом эквиваленте, что представляется актуальным в условиях возможного использования мусорных урн для размещения ВУ в террористических целях. Существующие конструкции урн, как правило, выполнены из металла, что приводит к повышению поражающего действия взрыва безо-

болочковых ВУ за счет фрагментации корпуса урны. Взрывобезопасная урна при взрыве в ней безоболочкового взрывоопасного предмета осколков не образует и снижает фугасное действие до безопасного уровня, а при взрыве осколочных боеприпасов обеспечивает надежное улавливание образующихся осколков наряду со снижением фугасного действия. Кроме того, такая урна может быть использована при обезвреживании обнаруженных и идентифицированных взрывоопасных предметов: этот предмет может быть накрыт урной или помещен в нее.

Эластичные контейнеры предназначены для снижения разрушительных последствий взрыва, в том числе: для поглощения осколков ВУ и снижения термобарического воздействия энергии взрыва на биологические и небиологические материальные объекты. Благодаря эластичности стенок контейнера исключается образование вторичных поражающих осколков при разрушении контейнера. Эластичные контейнеры заполняются водой или полужидкой средой, например, в виде геля.

При взрыве ВУ оболочка эластичного контейнера деформируется равномерно. По достижении предельной деформации эластичной оболочки происходит ее разрыв, фрагментация составляющих контейнера и формирование ударной волны. Энергия взрыва затрачивается на разрушение контейнера, разгон его фрагментов и жидкости. При этом значительно снижается давление в ударной волне, термическое воздействие и дальность разлета осколков ВУ.

Недостатки эластичных контейнеров: изделие, значительно снижая поражающие факторы взрыва – полностью не устраняет их воздействие; специалисты-взрывотехники могут анализировать ВУ, находящееся в контейнере, только дистанционно (например, используя досмотровые интроскопы различного типа).

Эластичные контейнеры для локализации действия взрыва широко используются службами безопасности США, Израиля, Великобритании, ЮАР и других стран. Также и в нашей стране.

Различных устройств и изделий, предназначенных для локализации взрывов на сегодняшний день достаточно много разработано как в нашей стране, так и за рубежом. Однако, как мы можем сделать вывод из проведенного анализа различных анти-

террористических средств, используемых для локализации последствий взрывов и иных поражающих факторов, данные изделия не идеальны. Они не могут полностью нейтрализовать последствия взрыва и полностью минимизировать тот вред, который может быть им нанесен.

Различными институтами и научно-производственными учреждениями ведутся разработки в данной области, которые впоследствии могут изменить данную ситуацию в лучшую сторону.

Бондаренко А.А.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Модель угроз безопасности персональных данных и ее обеспечение в ОВД России

Статья посвящена вопросам определения понятия модели угроз безопасности персональных данных и ее назначению. Для начала хотелось бы раскрыть понятие персональные данные. В Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» под персональными данными следует понимать любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Под обработкой персональных данных следует понимать любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу

(распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных.

На наш взгляд необходимо выделить в отдельную группу автоматизированную обработку персональных данных, то есть с использованием средств вычислительной техники и автоматизированных систем.

Персональные данные циркулируют в информационной системе персональных данных, под которой понимается совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Перейдем к рассмотрению понятия угрозы безопасности информации (персональным данным). В документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» дано следующее определение:

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Угроза будет реализована когда она соответствует уязвимости (слабому месту, «бреши» в системе защиты.

Далее рассмотрим, для чего необходимы модели угроз безопасности персональным данным. В общем случае, под моделью понимается объект, имитирующий свойства другого объекта и используемый для его исследования. Моделировать угрозы безопасности необходимо для того, чтобы избежать возможного ущерба при реализации угроз и принять превентивные меры по предотвращению угроз.

Проще говоря, модель угроз – это формализованное описание всех возможных угроз.

В ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» дано следующее определение модели угроз безопасности информации – физическое, математическое, описа-

тельное представление свойств и характеристик угроз безопасности информации.

Подводя небольшой итог можно сказать, что модель угроз – это документ, описывающий возможные угрозы безопасности персональных данных.

Модель угроз безопасности персональных данных необходима для определения требований к системе защиты. Без модели угроз невозможно построить адекватную (с точки зрения денежных затрат) систему защиты информации, обеспечивающую безопасность персональных данных. В систему защиты включаются только те средства защиты информации, которые нейтрализуют актуальные угрозы. В соответствии с пунктом 2 статьи 19 ФЗ «О персональных данных», обеспечение безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз.

Модель угроз разрабатывается лицами, ответственными за защиту персональных данных. Они могут пользоваться помощью сторонних экспертов. Разработчик должен владеть полной информацией об информационной системе персональных данных, знать нормативную базу по защите информации.

Порядок разработки модели угроз определен в документах ФСТЭК:

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» - данная модель содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» - данный документ содержит алгоритм оценки угрозы путем несложных расчетов, определяя статус каждой вероятной угрозы.

Для обеспечения защиты персональных данных в ОВД была разработана Инструкция по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации, утвержденная Приказом МВД РФ от 6 июля 2012 г. N 678 "Об утверждении Инструкции

по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации".

В данной инструкции указано, как следует организовать работу по обеспечению персональных данных при их автоматизированной обработке. Так же указано как следует организовать работу разрешительной системы доступа к информационной системе персональных данных. Определены обязанности должностных лиц органов внутренних дел Российской Федерации по защите персональных данных.

Подводя итог, хочется отметить, что в наше время наши персональные данные становятся более доступными, а следовательно и более уязвимыми. Это происходит из-за того, что огромное количество людей регистрируются в различных социальных группах, тем самым выдавая свои личные данные и сами подвергают их угрозе.

Именно из-за данной проблемы следует уделить много времени для разработок более надежных и актуальных моделей угроз безопасности персональным данным, а разрабатывать их нужно, как можно чаще, так как злоумышленники находят все новые пути обхода защиты.

Варквасова С.А.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Состояние информационной безопасности Российской Федерации основные задачи по ее обеспечению

Информационная безопасность (ИБ) не имеет точного определения и не имеет в литературе единого предмета исследования. Каждым автором термин «информационная безопасность» определяется по-своему.

Предмет информационной безопасности значительно шире предмета защиты информации. Об этом можно судить из определений, взятых из нормативно-правовых актов. Так, например, определение понятия «безопасность» в Доктрине информационной безопасности РФ, которое следует из определения в федеральном законе «О безопасности» от 5 марта 1992 года:

«Безопасность — состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» .

«Информационная безопасность РФ — состояние защищенности ее национальных интересов в информационной сфере, определяющейся совокупностью сбалансированных интересов личности, общества и государства.»[1]

Положение дел информационной безопасности в Российской Федерации требует безотлагательного решения следующих проблем:

- Развития научно-практических основ информационной безопасности, отвечающей современной геополитической ситуации и условиям политического и социально-экономического развития России.

- Формирования законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, предприятий, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.

- Разработки механизмов реализации прав граждан на информацию и информационную безопасность.

- Формирования системы информационной безопасности, являющейся составной частью общей системы национальной безопасности страны.

- Разработки современных методов аудита безопасности информационной системы, обеспечивающих комплексное решение задач защиты информации.

[1] http://psyfactor.org/lib/styugin6.htm

- Разработки критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.

- Исследований форм и способов цивилизованного воздействия государства на формирование общественного сознания[1].

Решение вышеперечисленных проблем информационной безопасности должно осуществляться на основе соответствующей государственной политики.

Таким образом, проблема обеспечения информационной безопасности принадлежит к числу проблем, без решения которых невозможен полномасштабный и эффективный переход к открытому информационному обществу.

Состояние информационной безопасности в России показывает, что уровень информационной безопасности в настоящее время не соответствует жизненно важным потребностям личности, общества и государства. Сегодняшние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение. Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит ко многим негативным последствиям.

Информационная безопасность является составляющей общей безопасности и стремительно развивается как во всем мире, так и в Российской Федерации, глобальная информатизация охватывает все сферы государства – экономическую, военную, политическую, промышленную и т.п. Кроме всего, вычислительная техника становится неотъемлемой частью жизнедеятельности человека.

В последние годы реализованы некоторые практические меры по укреплению информационной безопасности в Российской Федерации. Осуществлен ряд мероприятий по совершенствованию информационной безопасности в органах государственной власти и управления, в государственных организациях и на пред-

[1]http://www.rusarticles.com/bezopasnost-statya/sovremennoe-sostoyanie-informacionnoj-bezopasnosti-v-rossijskoj-federacii-5421983.html

приятиях. Успешному решению ряда вопросов информационной безопасности способствует создание Государственной системы защиты информации в России от иностранных технических разведок и от ее утечки по техническим каналам, а также систем лицензирования деятельности предприятий в области защиты информации и сертификации средств защиты информации.

Васорина Л.М.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Применение металлоискателей в борьбе с террористическими угрозами

Тема борьбы с терроризмом в настоящее время настолько актуальна, что приведение любых дополнительных аргументов в пользу ее изучения просто излишне.

В современных условиях терроризм представляет серьёзную угрозу безопасности не только государству, но и всему мировому сообществу. В борьбе с этим опаснейшим злом должны быть реально задействованы все государственные структуры различных ведомств, органов и подразделений. Главная задача террористов – запугать мир на столько, чтобы подчинить его; если это не возможно, то уничтожить мир.

События в современном мире позволяют говорить о новом, исключительно опасном виде преступного насилия - террористической войне. Ее особенность заключается в том, что она ведется не страной, государством, а террористической организа-

цией, хотя нередко при поддержке и попустительстве государства[1].

Проблемы борьбы с терроризмом пытаются решить ученые, имеющие глубокие познания в различных областях общественно-политической деятельности. Однако существенного снижения количества актов терроризма пока не зафиксировано.

В настоящее время, по мнению ряда экспертов, в мире действует около 500 террористических организаций. За последние 10 лет ими совершено 6500 актов международного терроризма, от которых погибло 5 тыс. человек и 11,5 тыс. пострадало.

В этих условиях меры противодействия террористам, в том числе профилактического характера, должны быть как никогда эффективными. Проблема решения задач уголовного судопроизводства (с точки зрения раскрытия) приобретает особую значимость и актуальность при выяснении (устранении) причин и условий совершенных преступлений.

В реальности это не всегда удается сделать в силу целого ряда причин, одна из которых — отсутствие единого унифицированного определения понятия «терроризм», наполненного конкретным содержанием в виде четко обозначенных признаков его состава как одного из преступлений.

Наибольшее распространение в России получили следующие способы актов совершения терроризма: угрозы по телефону (телефонный терроризм), демонстративная закладка муляжей взрывчатых веществ и взрывных устройств, скрытая закладка бомбы на объекте и ее взрыв, взрыв припаркованного автомобиля с взрывчатым веществом (далее ВВ), взрыв движущегося автомобиля с ВВ террористом-смертником, подбрасывание закамуфлированных под боевые предметы мин-ловушек в расчете на любопытство и беспечность граждан, засылка конкретному адресату бомбы в почтовом отправлении, захват и удержание заложников с использованием оружия и взрывного устройства (далее ВУ)[2].

---

[1]Авдеев Ю.И. Особенности современного международного терроризма и некоторые правовые проблемы борьбы с ним // Российская Федерация сегодня. 2009 - № 20.с.125

[2]Гушер А.И. Проблема терроризма на рубеже третьего тысячелетия новой эры человечества // Знание-сила. 2011 - № 12. С. 36.

Вместе с тем очевидно и то, что без объединения усилий в рамках единого оперативного замысла, выработки конкретных совместимых мер на основе четко выстроенной системы, имеющей общие ориентиры в форме конкретных целей и задач, соотнесенных между собой по способам деятельности и субъектам, могущим придать ему некий логически завершенный вид, эффективная борьба с терроризмом невозможна.

Современная наука большую роль отводит исследованию технико-криминалистических средств и методов борьбы с терроризмом. Использование специальных познаний в этой сфере способствует более тщательной разработке планов по борьбе с терактами.

Для непосредственной борьбы с терроризмом на различных его этапах привлекаются, как правило, органы управления и структурные подразделения следующих министерств и ведомств РФ. Широко в борьбе с террористическими угрозами применяются современные металлоискатели.

О том, что за такое устройство металлоискатель стало известно совсем недавно, буквально в начале 19 века. Именно в этот период это устройство было изобретено в США. Изначально металлоискатели использовались в крупных промышленных предприятиях для предотвращения воровства готовых деталей и металлических заготовок[1]. Спустя совсем короткое время они обрели широкое применение и в других сферах деятельности человека. Особо сильно ими начали интересоваться в сфере обеспечения безопасности. Арочные металлоискатели используются во всех аэропортах мира. А после того как появилась более компактная ручная версия металлодетектора, она стала обязательным атрибутом всех служб безопасности государственных и частых охранных органов.

Данные технические средства дают возможность осуществлять поиск монет, ювелирных украшений, кладов, оружия, реликвий и артефактов, а также исследовать места бывших боевых действий. Кроме того, металлоискатель можно использовать в

[1]Емельянов В.П. Проблемы ответственности за международный терроризм. - М., 2008. С. 21.

системах безопасности для обнаружения огнестрельного и холодного оружия или металлических изделий, похищаемых с производства, а также применять в промышленности для поиска металлических предметов в продукции и сырье; для локализации труб, кабельных трасс и пустот[1]. Данные технические средства, используемые для борьбы с террористической деятельностью, можно условно разделить на группы средств предупреждения террористических актов и средств, используемых при ликвидации последствий этих актов. Приборы и системы контроля персонала, посетителей и их ручной клади:

- стационарные металлоискатели - Поиск-ЗМ или Поиск-ЗМР и портативные ручные металлоискатели Сфинкс ВМ-611. Применяются для выявления холодного и огнестрельного оружия, металлических элементов взрывных устройств, скрытых под одеждой персонала и посетителей, в строительных конструкциях и мебели, при проверке объекта. Сигнализация световая и звуковая;

- ручной металлодетектор SUPER SCANNER является классическим досмотровым металлоискателем, пользующимся наибольшей популярностью у сотрудников правоохранительных органов и служб безопасности. Звуковой и световой сигнал тревоги при обнаружении металла на теле объекта. Максимальная глубина обнаружения, см: пистолет средних размеров - 23; бритвенное лезвие - 7,5. Несмотря на разнообразие данных средств электромагнитные помехи вызывают нарушение работы аппаратуры или даже не позволяют ее наладить в конкретном месте. Источниками таких помех могут быть распределительные щиты, мощное электротехническое оборудование, компоненты компьютерных сетей, наконец, влияние других подобных поисковых приборов, установленных на недопустимо близком расстоянии[2].

Металлоискатели и металлодетекторы используются при предупреждении подготавливаемых террористических акций в местах работы и постоянных маршрутов передвижения охраняе-

[1] Будницкий О.В. Терроризм в российском освободительном движении - М., 2012.с.58

[2] Федоров С.Г. Терроризм: реальность сегодняшнего состояния. - М., 2012. С. 64.

мых лиц, проведения съездов, собраний, торжественных заседаний, посредством осуществления следующих мероприятий:

- досмотр сотрудников и других лиц, посещающих режимные объекты государственных предприятий, учреждений и организаций, работниками военизированной охраны;

- «зачистка» помещений и территорий парков, стадионов, жилых зданий, киноконцертных залов, театров и других мест массового скопления людей при проведении там мероприятий[1].

Несмотря на то, что существуют различные металлоискатели и металлодетекторы это не решает проблемы нарастающей террористической угрозы. Несомненно, все эти средства помогают для распознания террористических актов, но в полной мере не решают данную проблему. Для успешной разработки способов предотвращения и методики расследования терроризма необходимо изучить практику деятельности специальных международных организаций, действующих в сфере расследования и предотвращения террористических акций, опыт сотрудничества правоохранительных органов и спецслужб России с соответствующими ведомствами зарубежных государств и средствами массовой информации.

В заключение следует сказать, что общество обязано искать противоядие террору, эффективно противостоять ему совместными усилиями профессионалов и обывателей, всех и каждого, и альтернативы нет[2].

---

[1] Федеральный закон от 06.03.2006 N 35-ФЗ (ред. от 23.07.2013) «О противодействии терроризму»

2 Авдеев Ю.И. Особенности современного международного терроризма и некоторые правовые проблемы борьбы с ним // Российская Федерация сегодня. 2009 - № 20.с.125

Гаврилов И.К.,
курсант 2курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Анализ видов информации ограниченного доступа, циркулирующей в органах внутренних дел

Федеральный закон РФ от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет деление информации (в зависимости от категории доступа к ней) на общедоступную информацию и информацию, доступ к которой ограничен федеральными законами (Ст.5). В той же статье информация классифицируется по способу распространения. Важным здесь является обособление информации, которая в соответствии с федеральными законами подлежит предоставлению или распространению. Т.е. доступ к этой информации ограничивать противозаконно.

Анализ показал, государственная тайна является самым защищаемым видом информации ограниченного доступа. Регулирование вопросов, связанных с этим видом тайн возложено на Закон РФ от 21 июля 1993 г. N 5485-I «О государственной тайне». Перечень сведений составляющих государственную тайну определен в ст. 5, где они сгруппированы по следующим направлениям:

сведения в военной области;

сведения в области экономики, науки и техники;

сведения в области внешней политики и экономики;

сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму.

Рассмотрим, с какой информацией ограниченного доступа сталкиваются в своей деятельности сотрудники органов внутренних дел.

Согласно п.п. 6 п. 1 ст. 28 ФЗ «О полиции» сотрудник полиции имеет право на доступ в установленном порядке к сведениям, составляющим государственную и иную охраняемую законом тайну, если выполнение служебных обязанностей по замещаемой должности связано с использованием таких сведений.

П. 4 ст. 5 ФЗ от 21.07.1993 № 5485-1 «О государственной тайне» относит к государственной тайне сведения о силах, средствах, об источниках, о методах, планах и результатах оперативно-розыскной деятельности, о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими оперативно-розыскную деятельность. Эти сведения конкретизируются в перечне, утвержденном Указом Президента Российской Федерации от 30.11.1995 № 1203 и ведомственном перечне, утвержденном приказом МВД.

Ст. 8 ФЗ от 07.02.2011 «О полиции» гласит, что деятельность полиции является открытой для общества в той мере, в какой это не противоречит требованиям законодательства Российской Федерации об уголовном судопроизводстве, о производстве по делам об административных правонарушениях, об оперативно-розыскной деятельности, о защите государственной и иной охраняемой законом тайны, а также не нарушает прав граждан, общественных объединений и организаций.

Оперативно-розыскная деятельность основывается на конституционных принципах законности, уважения и соблюдения прав и свобод человека и гражданина. Поэтому в ходе осуществления оперативно-розыскной деятельности должны соблюдаться требования 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). Вместе с тем Конституция РФ предусматривает ограничение прав и свобод человека и гражданина федеральным законом, но только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов дру-

гих лиц, обеспечения обороны страны и безопасности государства (ст. 55).

Порядок обращения со служебной информацией ограниченного распространения (составляющей служебную тайну) в федеральных органах исполнительной власти осуществляется в соответствии с Постановлением Правительства РФ от 03.11.1994 N 1233 и ведомственными инструкциями. В соответствии с указанным постановлением к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью. Носители информации, составляющей служебную тайну, имеют пометку «для служебного пользования». Правовой статус служебной тайны не совсем однозначный. Это объясняется тем, что в соответствии с ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» доступ к информации должен ограничиваться федеральными законами. После отмены с 01.01.2008 Федеральным законом от 18.12.2006 N 231-ФЗ статьи 139 «Служебная и коммерческая тайна» части первой Гражданского кодекса от 30.11.1994 № 51-ФЗ ни одним Федеральным законом доступ к служебной тайне не ограничивается. Но ведомственными нормативными документами определяется перечень сведений, отнесенных к служебной тайне и порядок постановки пометки «для служебного пользования» на носители такой информации, установлен специальный режим хранения и доступа. При приведении к присяге каждый сотрудник клянется хранить служебную тайну.

Служебная информация предоставляется сотрудником органов внутренних дел в рамках должностной компетенции только по официальным запросам в установленном порядке с разрешения руководства.

В статье 161 Уголовно-процессуального кодекса РФ от 18.12.2001 № 174-ФЗ говорится о недопустимости разглашения данных предварительного следствия. Они могут быть преданы гласности лишь с разрешения следователя или дознавателя. Разглашение данных о частной жизни участников уголовного судопроизводства без их согласия не допускается. Ст. 6 Кодекса про-

фессиональной этики сотрудника органов внутренних дел (утв. приказом МВД России 24.12.2008 № 1138) указывает на недопустимость разглашения фактов и обстоятельств частной жизни, ставших известными в ходе следственных действий.

Кроме того, органы внутренних дел в процессе повседневной оперативно-служебной деятельности получают доступ к персональным данным граждан, которые охраняются ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных». Персональные данные это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

В соответствии с п.п. 29 п. 1 ст. 13 ФЗ от 07.02.2011 «О полиции» сотрудникам полиции для выполнения возложенных на них обязанностей предоставляется право получать в целях предупреждения, выявления и раскрытия преступлений в соответствии с законодательством Российской Федерации сведения, составляющие налоговую тайну. Ч. 3 ст. 102 Налогового кодекса определяет, что поступившие в органы внутренних дел, сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа.

В результате анализа информации ограниченного доступа, которая находится в распоряжении сотрудников органов внутренних дел, можно сделать вывод о том, что состав таких сведений достаточно разнороден, а объем таких сведений велик и необходимо проводить целенаправленную разъяснительную работу с сотрудниками по порядку и правилам обращения с носителями информации ограниченного доступа с целью недопущения утечки информации.

Гаркуша В.В.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Технические средства контроля и досмотра

Под досмотровым оборудованием понимается комплекс технических средств, используемый правоохранительными органами и службами охраны для контроля посетителей и пассажиров, а также их вещей (ручной клади, багажа и т.п.) при обеспечении безопасности различных учреждений, массовых мероприятий и общественного транспорта.

Потребность в создании досмотровой техники возникла после ряда террористических актов, захвата воздушных судов и других транспортных средств, повлекших за собой не только материальный ущерб, но и человеческие жертвы. Возникла необходимость контроля пассажиров, их ручной клади и багажа в целях недопущения возможности проноса оружия, взрывчатых средств и других предметов, которые могут представлять опасность[1].

В связи с этой проблемой во всех ведущих странах начались работы по созданию эффективной досмотровой техники и организации ее производства.

В СССР эта проблема возникла в 1978 г., когда в рамках подготовки к Московской Олимпиаде было обнаружено, что аэропорты страны, которые должны были принимать гостей и участников Олимпиады, не оборудованы средствами защиты от террористических и других вандальных актов.

За относительно короткое время по техническому заданию службы безопасности гражданской авиации отечественной компанией была проведена конструктивная разработка и обеспечен промышленный выпуск рентгенотелевизионных интроскопов

[1]Антонов К. А., Андрюшин О.Ф. Ахматов А.П.Этапы развития отечественной досмотровой техники // Специальная Техника – №2 – 2006

«Луч-1», в которых формирование рентгеновского изображения содержимого досматриваемых объектов, установленных на транспортере, производилось с помощью синхронного вращения рентгеновских генераторов и приемников. Установка этих рентгенотелевизионных интроскопов в олимпийских аэропортах позволила обеспечить безопасный прием, а затем и отправку зарубежных участников и гостей Олимпиады-80.

После проведения Олимпиады работы по совершенствованию и разработке технических средств досмотровой техники продолжились. Была поставлена задача не только повышения эффективности действия существующих средств и расширения условий их применения, но и поиска путей создания новых средств, которые позволили бы контролировать не только проносимые личные вещи и багаж, но и владельцев этих предметов.

Учитывая широту и разнообразие средств, используемых для осуществления террористических и бандитских акций, появилась необходимость обнаружения наряду со штатным огнестрельным и холодным оружием типа пистолетов, револьверов, толовых шашек, штык-ножей, финок и взрывчатых закладок, стреляющих ручек, различных заточек и других всевозможных стреляющих, колющих, режущих и взрывающихся предметов.

К досмотровому оборудованию относятся: стационарные и переносные (портативные) рентгенотелевизионные установки, различные металлодетекторы, от простейших ручных до арочных многозонных установок и специальных селективных устройств, технические эндоскопы и досмотровые зеркала. К досмотровому оборудованию так же следует отнести детекторы опасных жидкостей и паров взрывчатых веществ, а также детекторы часовых механизмов, как механических, так и электронных.

Можно выделить несколько групп, в которые могут быть объединены технические средства поиска диверсионно-террористических средств:

металлоискатели, основанные на вихретоковых и магнитометрических методах;

эндоскопы и досмотровые зеркала;

интроскопы различного вида и типа (рентгеновские, ультразвуковые, СВЧ, с источником радиоактивного излучения);

волновые камеры миллиметрового диапазона;

газоанализаторы (хроматографы, дрейфспектрометры);

детекторы состава веществ, основанные на ядерно-физических методах (нейтронный, фотоядерный, ядерно-магнитного и ядерно-квадрупольного резонансов и др.)

радиометрические и спектрометрические приборы поиска радиоактивных веществ;

средства обнаружения приемников радиоуправляемых взрывных устройств;

средства обнаружения временных замедлителей взрывных устройств.

системы обнаружения оптических устройств

Средства визуального контроля предназначены для обследования мест, осмотр которых невооруженным глазом затруднителен или невозможен. Средства визуального контроля можно разделить на специальные досмотровые зеркала, эндоскопы, специальные видеокамеры.

Снимки и видео можно просматривать на телевизоре или сохранять в виде файлов на компьютере.

Оптоволоконный эндоскоп состоит из объектива, совмещенного источником света, световода и окуляра. Основным элементом эндоскопа является световод, изготовленный из множество оптоволоконных нитей. Свет по оптоволокну распространяется за счет многократного переотражения от внутренних стенок оптоволокна. Это позволяет свету распространяться вдоль него даже если оно изогнуто. Светодовод является направляющей средой для световых волн. Объектив воспринимает световые лучи и проецирует их на вход световода. На противоположном конце световода расположен окуляр, через который можно производить непосредственное наблюдение. Большинство эндоскопов имеют возможность подключать к окуляру объектив фотоаппаратов или видеокамер для осуществления документирования процесса досмотра. Рабочая часть эндоскопа имеет систему управления, позволяющую оператору с помощью системы тросов изменять угол поворота объектива.

Телевизионные эндоскопы отличаются от оптоволоконных тем, что изображение воспринимается миниатюрной видеокамерой, с помощью которой преобразуется в электрический сигнал. Сигнал передается на приемную сторону по проводнику. Суще-

ствуют и беспроводные системы, в которых сигнал от видеокамеры передается по радиоканалу, а работа самой камеры управляется дистанционно. Цифровая платформа таких устройств позволяет достаточно легко документировать полученные изображения путем сохранения фотоснимков или видео, при этом текущие процессы будут отображаться на встроенном мониторе.

Досмотровые зеркала – вспомогательные технические средства, предназначенные для визуального осмотра мест, доступ к которым затруднен или ограничен: в помещениях, транспортных средствах, контейнерах с грузом на предмет обнаружения подозрительных предметов (ВУ, радиомаяков и других посторонних предметов). Наиболее часто досмотровые зеркала применяются для автомобильного транспорта: днищ, колесных арок и других труднодоступных мест. Типовой досмотровый комплект зеркал включает в себя набор сменных зеркал различных размеров и конфигурации и телескопическую штангу, на которой с помощью подвижных шарнирных соединений закрепляется осветитель и одно из зеркал. Осветитель в большинстве случаев светодиодный, за счет чего обеспечивается высокая яркость свечения и малое энергопотребление, что особенно важно в нестационарных условиях. Зеркала, входящие в досмотровые комплекты, имеют, как правило, круглую форму и размеры от 60-220 мм в диаметре, а также прямоугольную форму с двумя наиболее распространенными типоразмерами зеркал 50х90 мм и 60х110 мм.

В качестве основного наиболее информативного и эффективного инструмента для досмотра ручной клади и багажа используются различного типа рентгеновские или рентгенотелевизионные установки (РТУ) - интроскопы. Рентгенотелевизионные установки позволяют в режиме реального времени рассмотреть внутреннюю структуру контролируемого объекта, идентифицировать инородные включения или дефекты. Возможности рентгенотелевизионных систем позволяют обнаружить отдельные элементы оружия и взрывных устройств, контейнеры с опасными вложениями и другие запрещенные к провозу предметы.

Стационарные системы подразделяются на конвейерные (сканирующие) и флюороскопические, выполненные в виде рентгенозащитных камер. Конвейерные установки более распространены и имеют высокие характеристики по скорости и качеству

контроля. Скорость конвейерных лент достигает 20-25,5 см/сек, что обеспечивает контроль значительного количества людей в потоке. Основным потребителем таких систем являются аэропорты, международные морские и речные порты, а также пункты контроля почтовых отправлений. Мобильная аппаратура предназначена в основном для оснащения временных постов контроля и решения антитеррористических задач. Портативные РТУ применяются для обследования оставленных предметов, труднодоступных мест в зданиях, сооружениях, транспортных средствах, выявления предметов, запрещенных к перевозке.

Рентгеновское и гамма- излучения обладают одинаковой природой (это коротковолновое электромагнитное излучение с частотой от $3 \cdot 10^{16}$ Гц до $6 \cdot 10^{19}$ Гц и длиной волны 0,005 — 10 нм) и подчиняются одинаковым закономерностям при взаимодействии с веществом. Принципиальная разница между двумя этими видами излучений заключается в механизме их возникновения: рентгеновское излучение возникает при торможении в веществе высокоэнергетических электронов; гамма-излучение является продуктом перехода ядра атома из одного энергетического состояния в другое. В области энергий до сотен килоэлектронвольт (кэВ), обычно применяемых в досмотровой аппаратуре, рентгеновские и гамма кванты при прохождении сквозь вещество взаимодействуют с электронами атомных оболочек, поглощаясь (фотоэлектрический эффект) или рассеиваясь (так называемое комптоновское рассеяние). Одним из самых важных параметров рентгеноаппаратов является их чувствительность, определяемая в мировой практике как размеры уверенного обнаружения на экране устройства визуализации специального тест-объекта в виде эталонной медной проволочки определённого диаметра. Чувствительность флюороскопов определяется в основном двумя параметрами - интенсивностью излучения и эффективностью его регистрации рентгеновским экраном - и зависит от толщины и плотности контролируемого объекта.

Способность рентгеновского и гамма излучений проникать через объекты, по разному поглощаясь различными веществами, используется в установках прямого просвечивания. Типовая рентгеноскопическая установка прямого просвечивания состоит из рентгеновской трубки (излучателя), создающей излучение,

преобразователя теневого изображения, блока обработки и визуализации. Исследуемый объект помещается между излучателем и преобразователем. Проходя через него рентгеновские лучи теряют часть своей энергии и попадают на экран преобразователя.

Интенсивность лучей в различных областях экрана будет различной и зависеть от веществ, из которых состоит объект исследования. Таким образом, исследуемый объект отбрасывает «тень» на экран преобразователя. Экран преобразователя состоит из флюоросцентных вещества. Воздействие на него рентгеновских лучей вызывает свечения, причем яркость свечения зависит от энергии воздействующего излучения.

Все эти средства позволяют выявить и нейтрализовать террористические угрозы при определенных условиях. Реальная эффективность использования технических средств зависит от существующей технологии контроля и квалификации персонала, их использующего.

Глебченко А.С.,
курсант 2курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России
к.т.н., доцент

Организационно-технические способы защиты от перехвата информации конфиденциального характера

Мероприятия по защите информации конфиденциального характера от утечки по техническим каналам (далее - технической защите информации) являются составной частью деятельности органов внутренних дел и осуществляются во взаимосвязи с другими мерами по обеспечению их информационной безопасности.

Защита информации конфиденциального характера от утечки по техническим каналам должна осуществляться посредством

выполнения комплекса организационных и технических мероприятий, составляющих систему технической защиты информации на защищаемом объекте, и должна быть дифференцированной в зависимости от установленной категории объекта информатизации или выделенного (защищаемого) помещения.

Организационные мероприятия по защите информации от утечки по техническим каналам в основном основываются на учете ряда рекомендаций при выборе помещений для установки технических средств обработки информации (ТСОИ) конфиденциального характера и ведения переговоров, введении ограничений на используемые ТСОИ, вспомогательные технические средства и системы (ВТСС) и их размещение, а также введении определенного режима доступа сотрудников на объекты информатизации и в выделенные помещения.

Технические мероприятия по защите информации от утечки по техническим каналам основываются на применении технических средств защиты и реализации специальных проектных и конструкторских решений.

Техническая защита информации осуществляется подразделениями по защите информации или отдельными специалистами, назначаемыми для проведения таких работ. Для разработки мер по защите информации могут привлекаться сторонние организации, имеющие лицензии ФСТЭК или ФСБ России на право проведения соответствующих работ.

Для защиты информации рекомендуется использовать сертифицированные по требованиям безопасности информации технические средства защиты.

Перечень необходимых мер защиты информации определяется по результатам специального обследования объекта защиты, сертификационных испытаний и специальных исследований технических средств, предназначенных для обработки информации конфиденциального характера.

Уровень технической защиты информации должен соответствовать соотношению затрат на организацию защиты информации и величины ущерба, который может быть нанесен собственнику информационных ресурсов.

Защищаемые объекты должны быть аттестованы по требованиям безопасности информации в соответствии с нормативны-

ми документами ФСТЭК России на соответствие установленным нормам и требованиям по защите информации. По результатам аттестации дается разрешение (аттестат соответствия) на обработку информации конфиденциального характера на данном объекте.

Ответственность за обеспечение требований по технической защите информации возлагается на руководителей организаций, эксплуатирующих защищаемые объекты.

В целях своевременного выявления и предотвращения утечки информации по техническим каналам должен осуществляться контроль состояния и эффективности защиты информации. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Защита информации считается эффективной, если принятые меры соответствуют установленным требованиям и нормам. Организация работ по защите информации возлагается на руководителей подразделений, эксплуатирующих защищаемые объекты, а контроль за обеспечением защиты информации - на руководителей подразделений по защите информации.

Технические решения по защите информации от утечки по техническим каналам являются составной частью технологических, планировочных, архитектурных и конструктивных решений и составляют основу системы технической защиты конфиденциальной информации.

В органе внутренних дел должен быть документально оформлен перечень сведений, подлежащих защите в соответствии с нормативными правовыми актами, а также разработана соответствующая разрешительная система доступа сотрудников к такого рода сведениям.

При организации работ по защите утечки по техническим каналам информации на защищаемом объекте можно выделить три этапа:

первый этап (подготовительный, предпроектный);

второй этап (проектирование системы технической защиты информации);

третий этап (этап ввода в эксплуатацию защищаемого объекта и системы технической защиты информации).

Горбунов А.Н.,
старший преподаватель кафедры
оперативно-разыскной деятельности
в органах внутренних дел
Краснодарского университета МВД

Основные направления организации борьбы с молодежным экстремизмом в России

В современный период в России, да и во многих других странах заметно актуализировались проблемы в обществе и государстве, связанные с молодежным экстремизмом. Кроме того, это явление стало носить все более общественно опасный характер, а именно: увеличивается количество преступлений с участием несовершеннолетних, поднимается уровень насилия в молодежной среде, его проявления становятся более жестокими. Противодействие проявлениям экстремизма среди молодежи становится общегосударственной задачей, включающей в себя различные аспекты ее реализации.

Прокуроры систематически проводят проверки по исполнению законодательства об образовании и противодействии экстремистской деятельности с принятием мер реагирования по выявленным нарушениям. Особое внимание при этом уделяется региональным и муниципальным нормативным правовым актам, противоречащим положениям Конституции РФ[1] и федеральным законам, создающим угрозу возникновения очагов межнациональной напряженности, межрелигиозных конфликтов и терроризма в субъектах Федерации.

Экстремистское поведение молодежи - одна из наиболее актуальных социально-политических и правовых проблем. Состояние, уровень, динамика экстремизма молодежи широко обсуждаются в средствах массовой информации и в специальной литературе, выпускаются аналитические сборники.

Экстремизм, как правило, в своей основе имеет определенную идеологию. Признаки экстремизма содержат только такие идеологии, которые основаны на утверждении исключительно-

[1]Российская газета. 2009. 21 янв.

сти, превосходства либо неполноценности человека на почве социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии, а также идеи политической, идеологической, расовой, национальной или религиозной ненависти или вражды в отношении какой-либо социальной группы.

Национализм является одной из форм патриотизма. Поэтому отождествление понятий «национализм» и «национальный экстремизм» и употребление их как синонимов является недопустимым. Что касается понятий «экстремизм» и «экстремистская деятельность», то следует сказать о том, что в Федеральном законе «О противодействии экстремистской деятельности» они имеют неточный и размытый характер. Неточность формулировок безгранично расширяет понятие уголовно наказуемого деяния. Под данный «состав» могут быть подведены практически любые действия правозащитников: распространение листовок, написание книг политического или социального содержания, выступление на митинге, использование транспарантов и т.д.

Многие ученые подчеркивают, что в основе молодежного экстремизма лежит так называемый этноцентризм - совокупность групповых конфликтных представлений, эмоционально-чувственных состояний и идеология вражды между своей и другими группами. Субъектами - носителями этноцентризма (конфликтного этнического сознания) - являются разные молодежные сообщества, которые дифференцируются от других по этническим, религиозным, социальным и другим признакам и могут рассматривать себя как «мы», а других как «они». Позитивные характеристики своей группы резко подчеркиваются и преувеличиваются, а свойства других групп и их членов оцениваются по стандартам своей группы (часто не всегда объективно) и при этом могут принижаться. Эта идеология и установка постулирует неизбежность отчужденности, враждебности и взаимной агрессивности в отношениях между сообществами. Наряду с понятием этноцентризма в литературе, общественно-политической и идеологической практике используется ряд других терминов, которые или синонимичны, или очень близки по своему содержанию по-

нятию этноцентризма. Речь идет, прежде всего, о таких понятиях, как национализм и терроризм[1].

Особенности современного российского молодежного экстремизма[2]:

- активное участие молодежи в возрасте от 14 до 30 лет в организованных массовых экстремистских акциях и их объединение в неформальные молодежные организации (группировки) экстремистско-националистической направленности и экстремистские сообщества;

- расширение географии экстремистской угрозы в Российской Федерации и увеличение количества национальностей, социальных групп, молодежных субкультур и тому подобных жертв экстремизма;

- мотивированные убийства: совершаемые в Российской Федерации убийства граждан другой национальности или вероисповедания, иностранных граждан все больше приобретают серийный, более жестокий, изощренно-профессиональный, издевательский, ритуальный характер, а само совершение экстремистских деяний становится не просто занятием ради любопытства, а профессиональной деятельностью определенных групп лиц;

- стремление экстремистско-националистических движений вовлечь в свои ряды членов различных агрессивных молодежных субкультур, неформальных молодежных объединений, групп, движений, а также лиц, ранее судимых;

- наличие у неформальных молодежных организаций (группировок) экстремистско-националистической направленности признака вооруженности, в том числе наличие взрывчатых веществ.

К причинам, порождающим экстремистские настроения в молодежной среде, необходимо также отнести социально-политические:

---

[1]Фридинский С.Н. Молодежный экстремизм как особо опасная форма проявления экстремистской деятельности / С.Н. Фридинский // Юридический мир. - 2012. - № 6. - С. 23-25.

[2]Мусаелян М.Ф. Профилактика экстремизма - важнейшее направление противодействия экстремизму в Российской Федерации / М.Ф. Мусаелян // Адвокат. - 2013. - № 7. - С. 99.

- преобладание досуговых ориентаций над социально полезными;
- кризис школьного и семейного воспитания;
- криминальная среда общения;
- неадекватное восприятие педагогических воздействий;
- отсутствие жизненных планов.

Исходя из всех факторов, способствующих развитию экстремистской деятельности, можно предложить следующие методы для предотвращения экстремистских настроений среди молодежи[1].

В первую очередь необходимо уделять большее внимание детям и подросткам, по следующим причинам:

1. Агрессивное поведение с чертами расовой, этнической и религиозной неприязни возникает на ранних стадиях индивидуального развития, и если остается без должного внимания, то может закрепиться или обостриться по мере взросления индивида. Следовательно, чем скорее начнется работа с моделями агрессивного поведения, тем больше шансов избежать агрессивного поведения во взрослой жизни.

2. Серьезные формы насилия, распространенные среди подростков, причиняют вред большему количеству людей.

Большая доля актов насилия и нетерпимости происходит в стенах общеобразовательных учреждений, непосредственно за ее пределами, там, где дети и подростки проводят значительную часть времени и завязывают социальные отношения. Поэтому школы, вузы и центры дополнительного образования - это «горячие точки» агрессии и в то же время они выступают в качестве арены осуществления антинасильственных программ.

Такие программы со всей очевидностью показывают, что для борьбы с агрессией в общеобразовательных учреждениях требуется сочетание целого ряда методов.

В общеобразовательных учреждениях должна быть сформирована такая атмосфера, в которой:

---

[1]Мусаелян М.Ф. Криминологические особенности современного российского молодежного экстремизма / М.Ф. Мусаелян // Российский следователь. - 2012. - № 10 - С. 21-24.

1. Учителя и ученики признают акты жестокости, насилия и агрессии, относясь к ним со всей серьезностью, а, не считая их чем-то незначительным.

2. Случаи насилия и агрессии систематически отслеживаются.

3. Демонстрация жестокости единодушно отвергается учениками как недопустимая.

Предлагаются следующие методы решения данной проблемы:

1. Обучение персонала. Необходимо осведомлять преподавателей о психологических факторах и социальных факторах, способствующих участию в деструктивных группах, о структуре и методах действия групп, их основных опознавательных знаниях, а также о деятельности местных группировок.

2. Образовательные подходы. Среди мер, направленных на учащихся как потенциальных членов групп, широко используется «воспитание сверстников». Встречи с представителями «конструктивной молодежи» (спортсмены, талантливая молодежь).

3. Кодекс внешнего вида и поведения. Еще один распространенный элемент мер по предотвращению насилия - наложение ограничений на то, как учащиеся одеваются и как они себя ведут. В группировках часто разрабатываются системы символьной коммуникации, которые служат для укрепления внутригрупповой сплоченности и сигнализируют чужакам о враждебности. Например, «правые группы «Скинхедов» используют белые шнурки в своих тяжелых кожаных бутсах. Этим они выражают готовность к физической агрессии. Такие меры, как запрет на знаки отличия и запрещение использовать определенные словесные выражения, могут сделать присутствие членов группировки менее заметным и снизить уровень общения, основанного на членстве в группировке.

4. «Планы безопасности» - комплекс мер, позволяющий избежать насилия в школе: установление CCTV камер, аппаратуры просмотра местности, охраны. Это также поможет уберечь и от терроризма[1].

[1]Мусаелян М.Ф. Криминологические особенности современного российского молодежного экстремизма / М.Ф. Мусаелян // Российский следователь. - 2012. - № 10 - С. 21-24.

Помимо активных мер по обеспечению физической безопасности подростков и молодежи не стоит забывать и о духовном просвещении, которое, прежде всего, заключается в воспитании толерантности.

Важность формирования толерантных отношений у молодежи обусловлена тем, что вопрос об уровне толерантности российского общества является сегодня критически важным.

Обострение межнациональных конфликтов, усиление тенденций проявления ксенофобии - животрепещущие проблемы современной России. Сложная социально-экономическая обстановка, геополитические изменения и значительные миграционные потоки непосредственно влияют на общественное мнение в области межэтнических отношений.

Необходимо осуществлять спланированное воздействие на процесс формирования жизненных ориентаций молодежи и, собственно, на будущее тех народов, к которым эта молодежь принадлежит. Стоит обратить особое внимание на студентов педагогических учебных заведений, будущих учителей и наставников, которые и должны привить данные ценности детям. Сегодняшние дети - это будущие жители единого демократического государства, которое станет по-настоящему демократичным только в том обществе, где на всех уровнях сформированы и действуют толерантные отношения.

Что же подразумевает под собой толерантность. Энциклопедический словарь трактует ее как терпимость к чужим мнениям, верованиям, поведению. Таким образом, толерантность охватывает все стороны человеческих отношений: социально-экономические, политические, религиозные. Рассмотрим особенности влияния на формирование толерантности в обществе?

Во-первых, существуют экономические и социально-политические реалии, несомненно влияющие на степень толерантности общества. Большую роль играют определенные институты, которые через производство и распределение ценностей, как правило, упорядочивают и структурируют поведение индивидов и поддерживают общепринятые нормы поведения, создавая тем самым общепринятый потенциал в обществе.

Во-вторых, существует ощутимая нехватка специалистов и общеобразовательных предметов в школах и вузах, которые бы

усвоили общие представления о структуре современной культуры, о различии ментальностей и менталитетов.

Одним из методов предупреждения проявления экстремизма в молодежной среде должен стать диалог между разными общностями.

Диалог является краеугольным камнем глобального ответа на любого рода конфликты и насилие, прежде всего те, что основаны на фанатизме и нетерпимости. Поскольку этот диалог будет охватывать разные слои населения в разных уголках страны, призывы к конфликту будут встречены с призывом к компромиссу. Ненависть будет встречена толерантностью. Насилие - решимостью.

Диалог основан скорее на понимании того, что мы представляем множественность культур, а не на том, что мы все одинаковы и согласны друг с другом.

Идея о том, что есть лишь один народ, который знает правду, один ответ на мировые проблемы или одно решение, удовлетворяющее нужды населения на протяжении истории, приносила огромный вред. Когда разнообразие идентичности ставится под сомнение, когда отрицается какой-либо образ жизни, когда существует угроза фундаментальной свободе выбирать свой образ жизни, именно тогда неизбежны конфликт, насилие и страдание.

Для каждого общества роль такого события, как случай проявления национализма и ксенофобии, следует рассматривать как особый сигнал беспокойства и тревожности, так как за этим может следовать открытое противостояние, в том числе и вооруженное.

Мероприятия по противодействию экстремистской деятельности в субъектах Федерации проводятся в рамках реализации Целевой программы по профилактике экстремистской деятельности и терроризма: мероприятия информационно-пропагандистского направления, воспитательная работа с населением, в том числе направленная на профилактику проявлений экстремизма в молодежной среде[1].

[1]Фридинский С.Н. Молодежный экстремизм как особо опасная форма проявления экстремистской деятельности / С.Н. Фридинский // Юридический мир. - 2012. - № 6. - С. 23-25.

Например, Министерством образования и науки Кабардино-Балкарской Республики организованы конкурсы и олимпиады среди студентов учреждений среднего и высшего профессионального образования на тему профилактики экстремизма в молодежной среде, разработаны методические материалы и проведены в образовательных учреждениях занятия по разъяснению основ законодательства в сфере межконфессиональных, межнациональных отношений. Проведены циклы бесед и лекций, классные часы, направленные на развитие у учащихся толерантности в сфере межнациональных и межконфессиональных отношений.
В целях совершенствования работы по противодействию экстремистской деятельности и терроризму, взаимообмена, накопления и анализа информации при координационном совещании руководителей правоохранительных органов в регионах созданы постоянно действующие межведомственные рабочие группы по вопросам противодействия экстремистской деятельности и терроризму.
С участием органов государственной власти субъектов Федерации и местного самоуправления, органов прокуратуры, других правоохранительных органов, представителей учебных и научных учреждений, общественных, религиозных организаций практикуется проведение научно-практических конференций, семинаров-совещаний, заседаний «круглых столов», на которых обсуждаются вопросы противодействия экстремистской деятельности, в том числе проблемы молодежного экстремизма.

В то же время в последнее время наметились тенденции, которые могут повлечь за собой дестабилизацию в обществе. Наблюдается влияние приверженцев нетрадиционного ислама, которые проявляют активность и настойчивость в распространении своих взглядов.

Наиболее значимым дестабилизирующим фактором в современный период в общественной жизни страны является деятельность молодежных националистических и экстремистских группировок, а именно сторонников Движения против нелегальной иммиграции, «антифа», «скинхедов» и др.

«Антифа» - неформальное молодежное объединение, члены которого, прикрываясь идеями антифашистского движения, совершают преступления в отношении "скинхедов" и других националистических группировок. Несмотря на то, что эти группиров-

ки пока не многочисленны и есть только в крупных городах, их деятельность вызывает значительный общественный резонанс[1].

Как правило, "скинхеды", "антифа" и другие неформальные молодежные группировки совершают хулиганство, умышленное причинение телесных повреждений, побои, т.е. преступления, предусмотренные ч. 2 ст. 213, п. п. «а» и «б» ч. 2 ст. 115, п. п. «а» и «б» ч. 2 ст. 116 УК РФ. Эти преступления совершаются по мотивам идеологической вражды и ненависти в отношении членов противоборствующей группировки, а также лиц «неславянской национальности».

Также отмечаются проявления сторонников запрещенной судом общественной организации «Национал-большевистская партия» в различных регионах страны, которые активно участвуют в несанкционированных шествиях, митингах, распространяют листовки, материалы, литературу экстремистской направленности, в том числе с использованием ресурсов сети Интернет. Поэтому особую важность приобретает деятельность по своевременному предупреждению обострения межнациональных обострений.

В свою очередь, предупреждение межнациональных конфликтов представляет собой исключительно сложную задачу, поскольку это явление порождается многими социальными, политическими, психологическими, экономическими, историческими и иными причинами. Следовательно, такие причины должны быть объектами профилактического вмешательства со стороны органов государственной власти, правоохранительных - в особенности. Эффективность деятельности ОВД по предупреждению и пресечению противозаконных деяний на национальной почве будет достигнута, если государственные органы власти серьезно будут работать над вопросами разрешения накопившихся проблем.

[1]Фридинский С.Н. Молодежный экстремизм как особо опасная форма проявления экстремистской деятельности / С.Н. Фридинский // Юридический мир. - 2012. - № 6. - С. 23-25.

Горюн К.С.,
курсант 1 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Технические каналы утечки информации

В связи с постоянным развитием и совершенствованием технических средств, повсеместного распространения информационно-телекоммуникационных сетей и разнообразных каналов передачи той или иной информации, стала актуальной тема перехвата информации с различных технических каналов связи.

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику.

Под техническим каналом утечки информации понимают совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об одном объекте, и физической среды, в которой распространяются информационный сигнал.

Для передачи информации по любому техническому каналу (функциональному или каналу утечки) последний должен содержать три основные элемента: источник сигнала, среду распространения носителя и приемник.

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источника сигнала могут быть:

а) объект наблюдения, отражающий электромагнитные и акустические волны;

б) объект наблюдения, излучающий собственные (тепловые) электромагнитные волны;

в) передатчик функционального канала связи,

г) закладное устройство;

д) источник опасного сигнала;

е) источник акустических волн, модулированных информацией.

Так как информация от источника поступает на вход канала на языке источника (например, в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т.д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. Кроме того, он выполняет следующие функции:

– производит запись информации на носитель;

– усиливает мощность сигнала (носителя с информацией) до предусмотренных значений;

– генерирует поля (акустические, электромагнитные) или электрический ток, которые переносят информацию;

– обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.

Носителями информации являются материальные объекты, обеспечивающие запись, хранение и передачу информации в пространстве и времени. Носителями информации являются: люди, макротела, поля, микрочастицы (электроны).

Макротела являются наиболее долговременными носителями различных видов информации. Прежде всего, материальные тела содержат информацию о своем составе, структуре (строении), о воздействии на них других материальных тел. В настоящее время бумага еще является достаточно распространенным носителем семантической информации, однако четко прослеживается тенденция замены бумаги машинными носителями (магнитными, полупроводниковыми, светочувствительными и др.).

Как говорилось выше, носителями информации являются также различные поля. Из известных полей в качестве носителей применяются акустические, электрические, магнитные и электромагнитные (в радиодиапазоне, в диапазоне видимого и инфракрасного света). Информация содержится в значениях параметров полей. Если поля представляют собой волны, то информация содержится в их амплитуде, частоте и фазе.

Из многочисленных элементарных частиц в качестве носителей информации наиболее широко используются электроны, образующие статические заряды и электрический ток.

Другие носители, например, поля не имеют четких границ в пространстве, но в любом случае их характеристики измеряемы. Физическая природа носителя-источника информации, носителя-переносчика и носителя-получателя может быть, как одинаковой, так и разной.

С точки зрения защиты информации, ее источниками являются субъекты и объекты, от которых информация может поступить к несанкционированному получателю (противнику). Ценность этой информации определяется информированностью источника.

Среда распространения носителя - часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя с информацией. Основными, которые надо учитывать при описании среды распространения, являются:

а) физические препятствия для субъектов и материальных тел;

б) мера ослабления (или пропускания энергии) сигнала на единицу длины;

в) частотная характеристика (неравномерность ослабления частотных составляющих спектра сигнала);

г) вид и мощность помех для сигнала.

Приемник выполняет функции, обратные функции передатчика. Он производит:

а) выбор (селекцию) носителя с нужной получателю информацией;

б) усиление принятого сигнала до значений, обеспечивающих съем информации;

в) съем информации с носителя (демодуляцию, декодирование),

г) преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного восприятия ими.

Канал утечки информации отличается от функционального канала передачи получателем информации. Если получатель

санкционированный, то канал функциональный, в противном случае - канал утечки.

Если говорить о существующей классификации технических каналов утечки информации, то основным классификационным признаком будет являться физическая природа носителя. В нее входят:

1. оптический канал (электромагнитное поле в диапазоне 0.46-0.76 мкм (видимый свет) и 0.76-13 мкм (ИК-излучения));

2. акустический канал (механические акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц – 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в газообразной, жидкой и твердой средах);

3. радиоэлектронный канал (носителями информации являются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по проводникам);

4. материально-вещественный источник (носителями информации в данном случае являются обычные материальные вещества – бумага, электронные носители и т.п.).

По информативности каналы утечки делятся на информативные, малоинформативные и неинформативные. Информативность канала оценивается ценностью информации, которая передается по каналу.

По времени проявления каналы делятся на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер.Периодический канал утечки может возникнуть при условии, например, размещения во дворе не укрытой продукции, демаскирующие признаки о которой составляют тайну. К эпизодическим каналам относятся каналы, утечка информации в которых имеет разовый, случайный характер.

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем - по нескольким последовательным или параллельным каналам. Такие каналы утечки будут называться составными.

В последнее время, в связи с существенно возросшими объемами передаваемой по различным техническим каналам информации, направление науки изучающее вышеуказанные аспекты передачи информации и ее утечки является достаточно актуальным. Поэтому целью статьи явилось краткая систематизация существующих знаний в данной области.

Гурбанов Р.Р.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Инженерно-техническая укрепленность объектов ОВД

Основой обеспечения надежной защиты объектов от преступных посягательств является надлежащая инженерно-техническая укрепленность в сочетании с оборудованием данного объекта системами охранной и тревожной сигнализации. Системы контроля и управления доступом, охранного телевидения и оповещения применяются для усиления защиты объекта и оперативного реагирования.

В зависимости от значимости и концентрации материальных, художественных, исторических, культурных и культовых ценностей, размещенных на объекте, последствий от возможных преступных посягательств на них, все объекты, их помещения и территории подразделяются на две группы (категории): А и Б. Ввиду большого разнообразия разнородных объектов в каждой группе, они дополнительно подразделяются на две подгруппы каждая: АI и АII, БI и БII.

Объекты подгрупп АI и АII - это объекты особо важные, повышенной опасности и жизнеобеспечения, противоправные действия (кража, грабеж, разбой, терроризм и другие) на кото-

рых, в соответствии с уголовным законодательством Российской Федерации могут привести к крупному, особо крупному экономическому или социальному ущербу государству, обществу, предприятию, экологии или иному владельцу имущества.

Объекты подгрупп БI и БII - это объекты, хищения на которых в соответствии с уголовным законодательством Российской Федерации могут привести к ущербу в размере до 500 минимальных размеров оплаты труда и свыше 500 соответственно.

К внешнему рубежу охраны объекта относится ограждение.

Ограждение подразделяется на основное, дополнительное и предупредительное.

Ограждение должно исключать случайный проход людей (животных), въезд транспорта или затруднять проникновение нарушителей на охраняемую территорию, минуя контрольно-пропускной пункт (КПП). Ограждение должно выполняться в виде прямолинейных участков, с минимальным количеством изгибов и поворотов, ограничивающих наблюдение и затрудняющих применение технических средств охраны. К ограждению не должны примыкать какие-либо пристройки, кроме зданий, являющихся продолжением периметра. Окна первых этажей этих зданий, выходящих на неохраняемую территорию, должны оборудоваться металлическими решетками, а при необходимости - и металлическими сетками. Ограждение не должно иметь лазов, проломов и других повреждений, а также незапираемых дверей, ворот и калиток. Выбор конструкций и материалов основного ограждения объекта, обеспечивающих требуемую надежность защиты объекта.

Дополнительное ограждение должно устанавливаться для усиления основного ограждения.

Предупредительное ограждение должно быть просматриваемым и выполняться из штакетника, металлической сетки, гладкой или колючей проволоки или другого материала.

Ворота устанавливаются на автомобильных и железнодорожных въездах на территорию объекта. По периметру территории охраняемого объекта могут устанавливаться как основные, так и запасные или аварийные ворота.

Конструкция ворот должна обеспечивать их жесткую фиксацию в закрытом положении.

Ворота с электроприводом и дистанционным управлением должны оборудоваться устройствами аварийной остановки и открытия вручную на случай неисправности или отключения электропитания. Ворота следует оборудовать ограничителями или стопорами для предотвращения произвольного открывания (движения). Запирающие и блокирующие устройства при закрытом состоянии ворот должны обеспечивать соответствующую устойчивость к разрушающим воздействиям и сохранять работоспособность при повышенной влажности в широком диапазоне температур окружающего воздуха (минус 40 до +50 °С), прямом воздействии воды, снега, града, песка и других факторов. При использовании замков в качестве запирающих устройств основных ворот, следует устанавливать замки гаражного типа или висячие (навесные).

Калитку следует запирать на врезной, накладной замок или на засов с висячим замком. Усиление защиты калиток рекомендуется выполнять аналогично способам усиления дверей и их коробок

Объект, на котором установлен пропускной режим или планируется его введение, должен оборудоваться КПП для прохода людей и проезда транспорта. КПП должен обеспечивать необходимую пропускную способность прохода людей и проезда транспорта.

В зависимости от категории объекта на КПП рекомендуется предусмотреть:

– помещение для хранения и оформления пропусков (карточек);

– камеру хранения личных вещей персонала и посетителей объекта;

– комнату досмотра;

– помещение для сотрудников полиции и размещения технических средств.

Для прохода людей через КПП необходимо предусмотреть коридор, оборудованный турникетами.

Водопропуски сточных или проточных вод, подземные коллекторы (кабельные, канализационные) при диаметре труб или коллектора от 300 до 500 мм, выходящие с территории объектов подгруппы AI должны оборудоваться на выходе с охраняемого объекта металлическими решетками. Решетки должны изготов-

ляться из прутков арматурной стали диаметром не менее 16 мм, образующих ячейки размером не более чем 150 мм, сваренных в перекрестиях. В трубах или коллекторах большего диаметра, где есть возможность применения инструмента взлома, необходимо устанавливать решетки, заблокированные охранной сигнализацией на разрушение или открывание.

Воздушные трубопроводы, пересекающие ограждения периметра, должны оборудоваться элементами дополнительного ограждения: козырьком из колючей проволоки или инженерным средством защиты типа «Спираль АКЛ». Инженерное средство защиты «Спираль АКЛ» разворачивается по верху трубопровода или вокруг него.

Наружные и внутренние стены зданий, перекрытия пола и потолка помещений объектов должны быть труднопреодолимым препятствием для проникновения нарушителей и иметь соответствующий класс защиты от взлома, который достигается правильным выбором строительных материалов для их изготовления.

Усиление стен, перекрытий и перегородок металлическими решетками должно производиться по всей площади, устанавливаемыми с внутренней стороны помещения. Решетки (сетки) привариваются к прочно заделанным в стену на глубину 80 мм стальным анкерам диаметром не менее 12 мм (к закладным деталям из стальной полосы 100, 50, 6 мм, пристреливаемым четырьмя дюбелями), с шагом не более 500, 500 мм. После установки решетки (сетки) должны быть замаскированы штукатуркой или облицовочными панелями.

Двери объектов и их помещений, люки (далее - дверные конструкции) должны быть исправными, хорошо подогнанными под дверную коробку.

Дверные конструкции должны обеспечивать надежную защиту помещений объекта и обладать достаточным классом защиты к разрушающим воздействиям. Выбор конструкций и материалов дверей, оценка их устойчивости, а также способы усиления имеющихся на объекте дверных конструкций. Входные наружные двери на объект, по возможности, должны открываться наружу. Их следует оборудовать не менее двумя врезными (накладными) замками, установленными на расстоянии не менее

300 мм друг от друга или одним врезным (накладным) и одним висячим замками Двухстворчатые двери должны оборудоваться двумя стопорными задвижками (шпингалетами), устанавливаемыми в верхней и нижней части одного дверного полотна. Сечение задвижки должно быть не менее 100 мм, глубина отверстия для нее - не менее 30 мм.

Оконные конструкции (окна, форточки, фрамуги) во всех помещениях охраняемого объекта должны быть остеклены, иметь надежные и исправные запирающие устройства. Стекла должны быть жестко закреплены в пазах. Оконные конструкции должны обеспечивать надежную защиту помещений объекта и обладать достаточным классом защиты к разрушающим воздействиям. Выбор оконных конструкций и материалов, из которых они изготовлены.

Висячие (навесные) замки следует применять для запирания ворот, чердачных и подвальных дверей, решеток, ставень и других конструкций. Данные замки должны иметь защитные пластины и кожухи.

Таким образом инженерно-техническая укрепленность объекта является одним из важнейших элементов охраны, препятствующим незаконному проникновению, и как следствия мерой профилактики террористических проявлений.

Гусев Я.С.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Инспекционно – досмотровые комплексы в борьбе с террористическими угрозами

Все большая интеграция Российской Федерации в мировые экономические процессы влечет за собой и заметное увеличение грузопотока через ее территорию. Данный факт, естественно, отражается на работе таможенных органов, загрузка которых в этой

связи возрастает в несколько раз. Наибольшую трудность среди всех видов таможенного контроля представляет проверка содержимого крупногабаритных грузов и транспортных средств – авиационных, морских, железнодорожных контейнеров, грузовых автомашин, рефрижераторов. Таможенный контроль указанных объектов предполагает проведение целого комплекса трудоемких и длительных разгрузочно-погрузочных работ. Практика показала, что на проведения этих процедур для одного транспортного средства уходит 2-3 часа. Таким образом, большинство транспортных средств, следующих через границы России, проходят таможенное оформление только на основании представленных документов, фактически без необходимой реальной идентификации содержимого.

Решение этой проблемы руководство Федеральной таможенной службы (ФТС) нашло в применении разнообразных технических средств таможенного контроля (ТСТК). Актуальность создания таких комплексов очевидна.

Опыт мировой таможенной практики, изученный отечественными специалистами, показал, что наиболее эффективной техникой в настоящее время является инспекционно-досмотровые комплексы (ИДК), позволяющие за 3-5 минут без вскрытия и разгрузки транспортного средства получить его изображение и изображение перевозимых в нем товаров с характеристиками, позволяющими их идентифицировать. Также комплекс позволяет обнаруживать в конструкционных узлах транспортных средств предметы, запрещенные к перевозке.

В составе ТСТК выделяют 7 самостоятельных, но взаимосвязанных классов ТСТК.

Первый класс включает технические средства, предназначенные для оперативной диагностики документов, представляющих для таможенного оформления объектов, перемещаемых через таможенную границу, с целью выявления подделки (допечатка, дописка текста, подчистка, замена листов, подделка печатей, штампов, подписей).

Второй класс включает технические средства, предназначенные для дистанционной оперативно-технической инспекции объектов таможенного контроля, в процессе которой осуществляется интроскопия объектов с помощью ИДК, контроль объёмов

и количество стратегически важных сырьевых товаров и выявить среди них предметы таможенных правонарушений.

Третий класс включает в себя технические средства, необходимые для проведения таможенного поиска тайников и сокрытий, досмотра товаров и транспортных средств, а так же применение технических средств для отбора проб содержимого объекта таможенного контроля.

Четвёртый класс включает технические средства, которые обеспечивают выполнение оперативно-технических действий.

Пятый класс – ТСКТ, которые необходимы для таможенного оформления, перемещаемых через таможенную границу товаров и транспортных средств, включая наложенные на них и на документы средства таможенного обеспечения.

Шестой класс включает ТСТК, которые предназначены для выполнения функций визуального наблюдения за действиями лиц, находящихся в зонах таможенного контроля.

Седьмой класс включает ТСТК, которые обеспечивают получение данных о информации, перемещаемой через таможенную границу, с целью выявления материалов, запрещённых к такому перемещению.

Основная проблема, возникающая при внедрении комплексов в российскую практику, заключается в том, что на данный момент нет конкретной технологии, применения ИДК в российских условиях. В настоящее время существует проблема отсутствия специалистов, подготовленных к работе на ИДК.

В последние годы во многих регионах Российской Федерации резко возросла террористическая активность, что грозит стать глобальной угрозой. Наиболее привлекательными для террористов являются объекты транспортных средств, как наиболее уязвимые по сравнению с другими. Теракты на транспорте как правило сопровождаются большим количеством жертв, парализуют деятельность важнейших сфер экономики и дестабилизируют обстановку в обществе.

Нельзя не отметить огромную профилактическую роль используемых комплексов. Осознание того, что таможенники, вооруженные ИДК, в состоянии сорвать самый коварный план «нечистых на руку» участников ВЭД, не позволяет такие планы строить. Этим и объясняется снижение количества серьезных

правонарушений, которые выявлялись на первоначальном этапе применения комплексов.

Данное утверждение подтверждается различными фактами. В частности, проводимый ЮТУ анализ свидетельствует, что зачастую потоки товаров, перемещаемых через таможенную границу Таможенного союза, смещаются во временные периоды, когда ИДК не работает, или в те пункты пропуска, где ИДК не функционирует.

Таким образом, проведение таможенных осмотров с применением ИДК в настоящее время в большей степени является превентивной (предупредительной, предохранительной) мерой для снижения рисков нарушения таможенного законодательства.

Докумов Р.А.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Специальное вооружение ОВД

В 2011 году в России был принят Федеральный закон «О полиции», в соответствии с которым полиция предназначена для «…защиты жизни, здоровья, прав и свобод граждан Российской Федерации, иностранных граждан, лиц без гражданства, для противодействия преступности, охраны общественного порядка, собственности и для обеспечения общественной безопасности»[1].

Для выполнения вышеназванных функций сотрудникам полиции предоставляется возможность применять к лицам, злостно нарушающим общественный порядок, совершающим административные правонарушения и преступления, стоящие на вооружении органов внутренних дел (далее - ОВД) специальные средства. А также, что в последнее время довольно актуальна, реаль-

[1]См.: ст. 1 О полиции: федеральный закон от 07.02.2011 № 3-ФЗ [Консультант Плюс].

ная опасность для жизни и здоровья, которая может угрожать самим сотрудникам полиции. Таким образом, применение специальных средств и специального вооружения вполне оправдано.

Определений понятия «специальные средства ОВД» существовало до принятия вышеуказанного федерального закона достаточно много, но в соответствии с действующим законодательством остановимся на следующем определении: «Специальные средства - это совокупность технических устройств, приспособлений и материалов, состоящих на вооружении ОВД, применяемых сотрудниками органов внутренних дел и военнослужащими внутренних войск при выполнении ими обязанностей по обеспечению общественного порядка и общественной безопасности, а также в иных, предусмотренных законом случаях»[1].

Нормативными правовыми актами Правительства Российской Федерации утвержден Перечень специальных средств, состоящих на вооружении органов внутренних дел Российской Федерации, а также правила их применения. Приказами МВД России регламентируются порядок подготовки и аттестации сотрудников на право применения специальных средств, особенности применения конкретных изделий, а также порядок действий сотрудников после их применения.

В соответствии с указанной правовой базой в ОВД Российской Федерации и внутренних войсках МВД России (далее – ВВ МВД России) создается система специальных средств, способных обеспечить решение широкого круга задач по борьбе с правонарушениями и террористическим актам без тяжкого вреда здоровью подвергшихся воздействию людей и разрушений инфраструктуры, при обеспечении безопасности для законопослушных граждан, по обстоятельствам вовлеченных в ситуацию правонарушения (нарушения общественного порядка).

В соответствии ч. 2 ст. 21 ФЗ «О полиции» сотрудники полиции имеют право применять следующие специальные средства:

1. палки специальные (палки резиновые, палки универсальные специальные и т.п.);

[1]См.: Средства индивидуальной бронезащиты и специальные средства органов внутренних дел: учебное пособие / сост. А.Г. Александров, В.Н. Цимбал. – Краснодар, 2013.

2. специальные газовые средства (аэрозольные распылители высокого давления, газовые баллончики, ручные газовые гранаты, выстрелы и патроны с газовыми гранатами и т.п.);

3. средства ограничения подвижности (наручники разнообразных модификаций);

4. специальные окрашивающие и маркирующие средства (специальные химические вещества: кармин, родамин, рододендрон и т.п.);

5. электрошоковые устройства (электрошоковые устройства, автономные искровые разрядники);

6. светошоковые устройства (специальные лазерные фонари и т.п.);

7. служебные животные (розыскные, караульные, патрульные собаки; патрульные лошади и т.п.);

8. световые и акустические специальные средства (светозвуковые гранаты, выстрелы со светозвуковыми гранатами и т.п.);

9. средства принудительной остановки транспорта (шипованные ленты, противотаранные устройства и т.п.);

10. средства сковывания движений (средства сковывания биологических объектов);

11. водометы;

12. бронемашины (специальные полицейские машины, оперативно-служебные автомобили, бронетранспортеры и т.п.);

13. средства защиты охраняемых объектов (территорий), блокирования движения групп граждан, совершающих противоправные действия (армированные колючие ленты и т.п.);

14. средства разрушения преград (малогабаритные взрывные устройства и т.п.).

Рассмотрим вопросы применения специального вооружения.

К первой группе отнесем оружие не летального или не смертельного воздействия в отношении человека. Так, применение физической силы и специальных средств сотрудником полиции должно происходить с учетом создавшейся обстановки, характера и степени опасности действий лиц, в отношении которых они применяются. При этом сотрудник полиции обязан стремиться к минимизации любого ущерба. К вышеуказанному оружию можно отнести: палки специальные, специальные газовые

средства, электрошоковые устройства, светошоковые устройства, световые и акустические устройства, водометы.

Ко второй группе отнесем это же оружие, но применяемое в отношении тех или иных материальных объектов. К ним относятся: средства принудительной остановки транспорта, средства разрушения преград.

Указанное выше оружие не летального или не смертельного воздействия предназначено для активного наступательного воздействия путем контр нападения на человека для приостановки его физической активности либо для повреждения, разрушения материальных объектов, каких-либо предметов. Их применение влечет причинение физического и материального ущерба[1].

К следующей группе можно отнести специальные средства, которые направлены также на воздействие в отношении человека или групп граждан, однако наносят меньший вред, могут использоваться для ограничения подвижности, сковывания и блокирования движений. К ним относятся: средства ограничения подвижности, специальные окрашивающие средства, средства сковывания движений, бронемашины, средства защиты охраняемых объектов (территорий), блокирования движения групп граждан, совершающих противоправные действия.

Говоря об ответственности сотрудников полиции при применении специальных средств отметим, что в соответствии с ч. 9 ст. 18 ФЗ «О полиции» сотрудник полиции не несёт ответственность за вред, причинённый гражданам и организациям, если применение физической силы, специальных средств и огнестрельного оружия осуществлялось по основаниям и в порядке, которые установлены федеральными конституционными законами».

В соответствии с частью 3 указанной статьи в состоянии необходимой обороны, в случае крайней необходимости или при задержании лица, совершившего преступление, сотрудник полиции при отсутствии у него необходимых специальных средств или огнестрельного оружия вправе использовать любые подруч-

[1]См.: Сильников А.М. Виды специальных средств, состоящих на вооружении ОВД, и их классификация // Вестник Санкт-Петербургского университета МВД России, Вып. № 3 (51), 2011. – С. 68.

ные средства, а также применять иное не состоящее на вооружении полиции оружие.

Говоря о возможном причинении ущерба при применении специальных средств Закон обязывает сотрудника полиции оказать первую помощь гражданину, получившему телесные повреждения, а также принять меры по предоставлению ему медицинской помощи (часть 4 статьи 19 ФЗ «О полиции»). Первая помощь в данном случае состоит в перенесении пострадавшего в безопасное место, остановке кровотечения, обеспечении доступа воздуха.

Существующая практика разработки, принятия на вооружение ОВД и практическое применение специальных средств при соблюдении правил применения гарантирует сохранение жизни, здоровья и трудоспособности правонарушителей и граждан, по обстоятельствам, вовлеченным в ситуацию правонарушения, целостность зданий, сооружений и инфраструктуры городов, населенных пунктов и промышленных объектов.

Выбор сотрудниками полиции специальных средств, состоящих на вооружении ОВД, строгое соблюдение правовых норм, устанавливающих основания их использования, а также существующие запреты и ограничения по применению вышеуказанных средств, повышают эффективность подразделений ОВД.

Джалилов Г.Н.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Применение досмотровой техники в деятельности ОВД

В настоящее время в деятельности ОВД применяется широкий арсенал средств досмотровой техники, реализующий различные методы и обеспечивающей эффективный контроль при до-

смотре. Основным средством контроля людей являются стационарные и ручные металлоискатели. Системы, использующие обратно рассеянное рентгеновское излучение, позволяют выявлять скрытые на теле человека оружие, взрывчатку и наркотики.

В качестве основного наиболее информативного и эффективного инструмента для досмотра ручной клади и багажа используются различного типа рентгеновские или рентгенотелевизионные установки - интроскопы. Рентгенотелевизионные установки позволяют в режиме реального времени рассмотреть внутреннюю структуру контролируемого объекта, идентифицировать инородные включения или дефекты.

Эндоскопы обеспечивают решение многочисленных задач визуального контроля внутренних плоскостей различных полостей, ниш, осмотра труднодоступных мест, доступ к которым возможен через небольшие отверстия.

При разработке досмотровых систем применяются самые современные достижения науки и техники. В них используются перспективные комплектующие, и все изделия сертифицированы в России.

Для оснащения антитеррористических и специальных подразделений ОВД разработан модельный ряд рентгеновских интроскопов «Игла» различного назначения. Они предназначены для оперативного досмотра багажа и личных вещей, а также транспортных средств, обследования подозрительных предметов, в том числе в «полевых условиях».

Цифровые рентгеновские комплексы обеспечивают разрешение 30 мкм. Столь высокий показатель позволяет обнаруживать сотрудниками ОВД объекты тоньше человеческого волоса.

Освоенные в серийном производстве комплексы являются единственным из производимых в России типом портативных просвечивающих комплексов, которые позволяют работникам ОВД производить досмотр в условиях ограниченного доступа - достаточно всего 5 сантиметров свободного пространства за обследуемым предметом.

Наряду с досмотровой техникой отечественного производства в подразделениях МВД России всё большее применение находит и передовая зарубежная досмотровая техника. Охарактеризуем лишь некоторые ее технические средства.

Система Astrophysics XIS-Trailer предназначена для досмотра багажа и малогабаритных грузов, смонтирована на базе автомобильного прицепа и используется для организации мобильных пунктов досмотра. Туннель 1200 х 1010 мм.

Система Astrophysics XIS-Minivan используется для организации мобильных пунктов для досмотра багажа и мелких грузов. Система смонтированная на базе автомобиля. Туннель 1010 х 1010 мм.

Система Rapiscan Eagle® M4507 — уникальное соединение рентгена высокой энергии с эксплуатационной гибкостью всепогодной системы, способной обнаруживать запрещённые предметы и вещества на дорогах общего пользования. Дополнительно данная система оснащена детектором на обнаружение радиоактивных материалов. Проникновение по стали 300 мм.

Система Rapiscan VEDS MC Series — нейтронная система досмотра, которая автоматически обнаруживает наличие взрывчатых веществ и наркотиков в грузах. Система разработана для обнаружения значительного количества указанных опасных веществ, например широко применяемых в закладываемых в автомобиль бомбах или спрятанных в грузе.

Козловый сканер Rapiscan Eagle G60 на рельсовом ходу обеспечивает автоматизированное сканирование плотных и плотно упакованных грузов. Функция разделения материалов помогает сотруднику ОВД выявлять обладающие низкой плотностью запрещенные предметы, например взрывчатые вещества и наркотики.

Система Rapiscan VEDS GE Series — нейтронная система досмотра, которая автоматически обнаруживает наличие взрывчатых веществ и наркотиков в грузах. Система разработана для обнаружения значительного количества указанных опасных веществ, например широко применяемых в закладываемых в автомобиль бомбах или спрятанных в грузе.

Система Rapiscan Eagle T10 сканирует грузы при проезде автомобиля через портал, обеспечивая высокую пропускную способность. Система обеспечивает высочайшее качество построения изображения и имеет надежные стандартные функции. Rapiscan Eagle T10 монтируется на трейлере серийной и военной конфигураций.

Система ПРТУ 130100 (автотрейлер, оборудованный встроенным рентгенотелевизионным аппаратом Hi-Scan 130100) обычно используется при погрузке/разгрузке багажа или груза, который должен быть досмотрен в целях безопасности. Тоннель 1200 х 1010 мм.

Система Astrophysics XIS-Van предназначена для досмотра багажа и мелких грузов, смонтирована на базе автомобиля. Применяется для организации мобильных пунктов досмотра. Туннель 1010 х 1010 мм.

Система Rapiscan Eagle MSCS6000 — передвижной инспекционно-досмотровый комплекс досмотра грузов с источником излучения мощностью 6 МВ. Проникновение по стали 375 мм. Система обеспечивает сканирование 20-футового контейнера менее чем за 30 секунд.

Система Rapiscan GaRDS™ - наиболее современная, автономная, мобильная система досмотра грузовиков, грузовых контейнеров и пассажирского транспорта для выявления запрещенных предметов и взрывчатых веществ. Системы GaRDS отвечают требованиям США и международных стандартов по радиационной безопасности.

Козловый сканер Rapiscan Eagle G45 на рельсовом ходу обеспечивает высокоавтоматизированное сканирование плотных и плотно упакованных грузов. Он предоставляет возможность сканирования автомобиля с водителем благодаря технологии Rapiscan CabScan™ и имеет лучшее в своем классе качество построения изображения.

Система Rapiscan GaRDS Gantry — рентабельная, безопасная и надежная система досмотра грузовиков, транспортных средств и грузовых контейнеров с целью выявления запрещенных предметов, незадекларированных товаров и проверки соответствия груза грузовой декларации. Исрользуется как при таможенном досмотре, так и в подразделениях ОВД.

Система Rapiscan Eagle M 10 обеспечивает высочайшее качество построения изображения, имеет надежные стандартные функции и самые совершенные опции — все это делает ее наиболее удобной в пользовании и универсальной из всех мобильных систем в своем классе.

Применение в практической деятельности подразделений ОВД вышеуказанной досмотровой технике обеспечивает повышение раскрываемости преступлений, более эффективную борьбу с торговцами наркотиками и предотвращение террористических актов на территории.

Дубовикова А.В.,
курсант 1 курса
Краснодарского университета МВД России
Тхапшоков А.Ю.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Технические средства обеспечения безопасности информации

Развитие информационных технологий, средств беспроводной коммуникации, социальных сервисов, предназначенных для предоставления возможности общения людей, которые могут находиться на расстоянии друг от друга в сотнях, а то и тысячах километрах, все это по отдельности и в совокупности говорит о внедрении разнообразной информации в повседневную жизнь общества. Сейчас просто невозможно представить человека без мобильного телефона, компьютера и подобных устройств века XXI - информационного, как его теперь называют.

Информация находится вокруг нас, окружающее пространство просто пропитано всевозможными информационными полями (электромагнитными, оптическими, электрическими и т.п.), посредством которых происходит передача тех или иных данных.

В соответствии с действующим законодательством в области информации под этим термином понимаются: «…сведения (сообщения, данные) независимо от формы их представления»[1].

Происхождение термина «информация» связано со стремлением людей передавать друг другу различные сведения, необходимые им для жизни и осуществления различных видов деятельности. Таким образом, информация – это обобщенное понятие, включающее 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[2].

Следует отметить, что нередко информация является предметом преступного посягательства. Также информация используется и для раскрытия, расследования и предупреждения преступлений.

Однако рассмотрим еще несколько определений в области информации.

Под информационными технологиями понимаются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов[3].

Также достаточно часто используется термин «информационная система». Часто он рассматривается как в широком, так и в узком смысле.

В широком смысле: информационная система есть совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать надлежащих людей надлежащей информацией[4].

---

[1]См.: ст. 2 Об информации, информационных технологиях и о защите информации: федеральный закон от 27.06.2006 № 149-ФЗ.

[2]См.: Советский энциклопедический словарь / гл. ред. А.М. Прохоров. 4-е изд. - М.: Сов. энциклопедия, 1988. С. 499

[3]См.: Специальная техника органов внутренних дел: Часть 1. Учебник / под общ. ред. Ю.А. Агафонова. – Краснодар: КрУ МВД России, 2011. – С. 138.

[4]См.: Википедия. Свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Информационная_система#

cite_note-William_S._Davis.2C_David_C._Yen.E2.80.941998.E2.80.94.E2.80.94-1 (датаобращения: 19.01.2014).

Информационная система - автоматизированная система, результатом функционирования которой является представление выходной информации для последующего использования[1].

В узком смысле: информационная система – это программно-аппаратная система, предназначенная для автоматизации целенаправленной деятельности конечных пользователей, обеспечивающая, в соответствии с заложенной в неё логикой обработки, возможность получения, модификации и хранения информации[2].

Направления обеспечения безопасности информационных систем рассматривается как совокупность комплексных мер направленных на предотвращение угроз информационным системам на различных уровнях. При этом выделяют: правовое, организационное, инженерно-техническое направления обеспечения безопасности информационных систем.

Правовая защита информации заключается в разработке нормативных правовых актов, регламентирующих отношения, возникающих при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий и обеспечении защиты информации. В сфере защиты информации базовым законодательным актом является цитируемый нами выше Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. Данный нормативно-правовой акт регулирует отношения, связанные с осуществлением права на поиск, получение, передачу, производство и распространение информации; применением информационных технологий; обеспечением защиты информации.

Под организационной защитой понимается регламентация служебной деятельности и взаимоотношений сотрудников на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение информацией ограниченного доступа и проявление внутренних и внешних угроз.

---

[1]См.: ГОСТ РВ 51987-2002. Информационная технология. Комплекс стандартов на АС. Типовые требования и показатели качества функционирования информационных систем.

[2]См.: Маглинец Ю.А. Разработка информационных систем. Часть 1. Структурные методы. – Красноярск: Кларитеанум, 2004.

К основным организационным мероприятиям можно отнести:

– организацию режима и охраны с целью исключения возможности несанкционированного проникновения на территорию и в помещения посторонних лиц, контроля прохода на территорию сотрудников и посетителей;

– организацию защищенного документооборота;

– организацию работы по допуску сотрудников к информации ограниченного доступа;

– организацию использования технических средств сбора, обработки, передачи и хранения информации ограниченного доступа;

– организацию работы по анализу внутренних и внешних угроз информации ограниченного доступа;

– организацию работ по проведению систематического контроля за сотрудниками, работающими с документами ограниченного доступа.

Инженерно-техническая защита информации – это совокупность органов, специальных технических средств и мероприятий по их использованию с целью защиты информации ограниченного доступа.

По функциональному назначению средства инженерно-технической защиты информации возможно классифицировать на следующие группы:

1 физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям информации ограниченного доступа и осуществляющие защиту сотрудников, материальных средств и информации от противоправных воздействий.

В зависимости от значимости и концентрации материальных, художественных, исторических, культурных и культовых ценностей, размещенных на объекте, последствий от возможных преступных посягательств на них, все объекты, их помещения и территории подразделяются на две группы (категории): А и Б. Ввиду большого разнообразия разнородных объектов в каждой

группе, они дополнительно подразделяются на две подгруппы каждая: АI и АII, БI и БII.

Для каждой категории объектов, учитывая их функциональное назначение, существуют рекомендации МВД России по организации системы охранной безопасности. Также к обеспечению физической защищенности объектов используются системы контроля и управления доступом совместно с системой охранного телевидения, охранной и тревожной сигнализации.

2 аппаратные средства включают в себя приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации с целью гарантированной защиты информации от утечки, разглашения и несанкционированного доступа.

Каналы утечки информации по физической природе носителя разделяются на оптические, акустические, радиоэлектронные и материально-вещественные. Для того чтобы предотвратить утечки информации по разным каналам, используются различные технические устройства: генераторы акустического и электромагнитного шума, специализированные радиоукрытия, сетевые фильтры и т.п.

3 программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки данных.

К специализированным программам и программно-аппаратным комплексам, предназначенным для защиты данных от несанкционированного доступа можно отнести: программно-аппаратный комплекс «Соболь», система защиты информации «Secret Net», средство защиты информации «Аура», программное средство защиты информации от несанкционированного доступа в автоматизированных системах «Снег 2.0» и т.п.

4 криптографические средства с помощью специальных математических алгоритмов производят преобразование информации передаваемой по линиям связи или хранящейся в технических средствах таким образом, что при несанкционированном доступе злоумышленник не имеет возможность ознакомиться с содержанием передаваемой или хранимой информации.

Криптографическая защита информации является одним из эффективнейших решений для обеспечения безопасности данных. Доступ к зашифрованной информации может быть получен только в том случае, если лицо знает, как ее расшифровать, и поэтому хищение данных абсолютно бессмысленно для несанкционированного пользователя. К системам криптографической защиты могут быть отнесены: аппаратно-программный комплекс шифрования «Континент», персональное средство криптографической защиты информации «Шипка», средство криптографической защиты информации «КриптоПро CSP» и т.п.

Обеспечение безопасности передачи той или иной информации на сегодняшний день приняло достаточно актуальный характер. Если говорить об обычном человеке, то защита персональных данных, банковской информации и т.д. носит весьма важное значение в области обеспечения прав и свобод гражданина. Если говорить о системе правоохранительных органов, то не обеспечение безопасности свидетелей, потерпевших или иных участников предварительного расследования и уголовного судопроизводства; разглашение сведений о лицах, оказывающих содействие органам, осуществляющим оперативно-розыскную деятельность и т.п. может повлечь за собой причинение вреда жизни и здоровью граждан, «провалить» долгосрочные оперативно-следственные мероприятия, дать возможность лицам, причастным к совершению преступлений, избежать наказания.

Журтов К.А.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Сущность понятия «защита информации» и ее значение в обеспечении информационной безопасностью

Изначально под информацией понимались сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т.д.). С середины XX века к понятию информация добавились сведения, передаваемые между человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире, передача признаков от клетки к клетке, от организма к организму.

Сформулированные к настоящему времени строгие научные определения концентрируют внимание на одном из основных аспектов этого многозначного понятия — соотношении информации и материи.

Под информацией надо понимать сведения, являющиеся объектом сбора (накопления), хранения, обработки (преобразования), непосредственного использования и передачи.

Определению информации как сведений разного рода, представленных в любой форме и являющихся объектами различных процессов, наиболее соответствует следующая узкая трактовка понятия «защита информации».

В этом случае под защитой информации понимается совокупность мероприятий и действий, направленных на обеспечение ее безопасности, т.е. конфиденциальности, целостности и доступности. Это определение подразумевает тождественность понятий «защита информации» и «обеспечение безопасности информации».

Под защитой информации, в более широком смысле, понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Сущность защиты информации состоит в выявлении, устранении или нейтрализации негативных источников, причин и условий воздействия на информацию. Эти источники составляют угрозу безопасности информации. Цели и методы защиты информации отражают ее сущность.

В этом смысле защита информации отождествляется с процессом обеспечения информационной безопасности, как глобальной проблемы безопасного развития мировой цивилизации, государств, сообществ людей, отдельного человека, существования природы. При этом понятие информационная безопасность характеризует состояние(свойство) информационной защищенности человека, общества, природы в условиях возможного действия угроз и достигается системой мер, направленных:

– на предупреждение угроз, т.е. создание превентивных мер по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;

– на выявление угроз, что выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

– на обнаружение угроз, которое имеет целью определение реальных угроз и конкретных преступных действий;

– на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;

– на ликвидацию последствий угроз и преступных действий.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, многозвенной системы защиты физическими, техническими, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения информации о готовящихся противоправных актах, планируемых

хищениях, подготовительных действиях и других элементах преступных деяний.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке действий по нарушению безопасности информации.

Обнаружение угроз – это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.

Пресечение или локализация угроз – это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

– предотвращение разглашения и утечки конфиденциальной информации;

– воспрещение несанкционированного доступа к источникам конфиденциальной информации;

– сохранение целостности, полноты и доступности информации;

– соблюдение конфиденциальности информации;

– обеспечение авторских прав.

Учитывая вышесказанное защиту информации можно определить как совокупность методов, средств и мер направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов:

– обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;

– предотвращению утечки и утраты информации;

– сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;

– сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Зарудний Я.В.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Порядок работы с общедоступными персональными данными

В Федеральном законе Российской Федерации от 27 июля 2006 г. N 152-ФЗ дается определение понятиям персональные данные и общедоступные персональные данные:

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

В соответствии со ст. 8 ФЗ от 27.07.2006 № 152-ФЗ, для информационного обеспечения могут создаваться общедоступные источники персональных данных. В общедоступные источники персональных данных только с письменного согласия субъекта ПД могут вносится его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных

данных. Общедоступными признаются источники персональных данных, доступ к которым не ограничен и не требует получения предварительного согласия субъектов персональных данных. Общедоступные источники персональных данных могут использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Создание общедоступных источников персональных данных обусловлено необходимостью информационного обеспечения. Анализ действующего законодательства позволяет отметить, что к числу общедоступных источников персональных данных в настоящее время относятся: справочники, адресные книги, энциклопедии, документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющих общественный интерес или необходимых для реализации прав, свобод и обязанностей граждан. Например, ст. 29 Федерального закона «Об образовании в Российской Федерации» предписывает предоставлять информацию о руководителе образовательной организации, его заместителях, руководителях филиалов образовательной организации (при их наличии), а также о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы. Таким образом, при приеме на работу педагогического работника необходимо получить его согласие на включение необходимых данных в общедоступные источники.

Следует различать согласия на обработку персональных данных и согласие на включение персональных данных в общедоступные источники персональных данных. Согласие на обработку разрешает оператору обрабатывать персональные данные субъекта без нарушения их конфиденциальности. В случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

Необходимо помнить, что общедоступные сведения о субъекте персональных данных в любое время могут быть удалены из общедоступных источников персональных данных по требованию субъекта персональных данных, либо по решению суда или

иных уполномоченных государственных органов. Например, при увольнении педагогического работника он может потребовать удалить их с сайта образовательной организации. Этот факт обуславливает требование о необходимости защиты в том числе и общедоступных персональных данных.

Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» относит информационные системы, обрабатывающие общедоступные персональные данные к 4 уровню защищенности, который предусматривает:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Коваленко А.Н.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Состав и классификация носителей с защищаемой информацией в органах внутренних дел

Первоисточником термина информация является латинское слово informatio (изложение, истолкование, разъяснение), а вошло оно в русский язык в эпоху Петра.[1.]

На общелексическом, бытовом уровне понятие «информация» чаще всего толкуется как сведения, сообщения, передаваемые от человека человеку и осведомляющие о каких-то явлениях, событиях, процессах и т.д.

Норберт Винер определяет информацию как «обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления». Винер утверждает, что информация вне человеческого сознания не существует. Многие современные представления о содержании понятия «информация» связаны с человеком и его способностью мыслить.

«Информация – это сообщение, осведомляющее о положении дел, о состоянии чего-нибудь»[2].

Во всех случаях, когда идет речь о сведениях, следует понимать, что говорится об информации осмысленной, преобразованной человеческим сознанием. Согласно словарю В.И. Даля, слово «сведения» происходит от «сведать», т.е. узнать, получить сведения. Оно также является синонимом слов «знание», «известие», «уведомление»[3].

---

[1]Черных П.Я. Историко-этимологический словарь русского языка. М., 1993. С. 335.
[2]Ожегов С.И. Словарь русского языка. М., 1952. С. 220.
[3]Даль К.И. Толковый словарь живого великорусского языка. Т. 4. М., 1994. С. 155.

Отождествление информации со сведениями или фактами, которые теоретически могут быть получены и усвоены, т.е. преобразованы в знания, составляет суть антропоцентрического подхода к определению понятия «информация». Этот подход в настоящее время применяется наиболее широко и, в частности, в российском законодательстве.

До последнего времени антропоцентрический подход удовлетворительно работал в области правовых и общественных наук. Однако в связи с широким внедрением вычислительной техники его недостатки все чаще дают о себе знать.

Во-первых, подход к информации только как к сведениям не позволяет адекватно интерпретировать информационные процессы в таких объектах, как компьютерные программы, компьютерные сети, системы искусственного интеллекта, системы, ориентирующиеся в состоянии неопределенности. Здесь процессы получения, преобразования, передачи информации могут проходить без этапа осмысления их человеком.

Во-вторых, в рамках антропоцентрического подхода невозможно найти адекватного объяснения генетической информации живой природы.

В связи с этим возникла потребность в изменении трактовки понятия информации. Оно было расширено и включило обмен сведениями не только между человеком и человеком, но также между человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке. Наиболее бурное и весьма плодотворное развитие проблема проникновения в сущность понятия «информация» получила в рамках теории информации и кибернетики.

Теория информации начинается с работ К. Шеннона, опубликованных в конце 40-х гг. XX в., в которых под информацией понимались не любые сообщения, а лишь те, которые уменьшают неопределенность у получателя этого сообщения. В теории Шеннона на первый план выдвигалась идея кода и канала передачи информации, а количество информации, характеризующее данное сообщение, определялось множеством всех возможных сообщений и их вероятностей независимо от их смыслового содержания.

В начале 60-х гг. Ю.А. Шрейдер предпринял попытку разработать методы определения того, как богатство состава и структурность информации, накопленной в объекте, влияют на ее прием и эффективность обработки для использования. Так появилась семантическая теория информации, развитая Ю.А. Шрейдером1, которая отличается от теории информации К. Шеннона по своим исходным положениям. Чтобы вообще воспринять какую-либо информацию от внешних источников, система-приемник должна обладать неким минимальным «запасом знаний», который обозначается термином «тезаурус». Если позволяет эта пороговая информация, система способна расширять свой тезаурус, извлекая извне все более обширную информацию, вплоть до максимально для нее доступной, когда ее внутренняя информация (тезаурус) обогащается до оптимального уровня. Дальнейшее восприятие информации становится для системы все более избыточным (все менее значимым) и, наконец, она уже «знает все, что ей доступно. Описанную схему Шрейдер поясняет на примере восприятия информации человеком: если, например, источник внешней информации – учебник по теории вероятностей, то школьник младших классов не извлечет из него никакой информации (его начальный тезаурус для этого недостаточен), школьник старших классов уже извлечет некоторую информацию, а студент, изучающий этот курс, – максимальную.

С точки зрения обеспечения информационной безопасности под понятием «носитель» необходимо понимать какой-то объект, обладающий определенной информацией, которую можно получить (получать) одноразово или многократно интересующимися ею лицами. Носитель связан с каким-то получателем (субъектом), имеющим ту или иную возможность доступа к информации. Тогда под носителем конфиденциальной информации будем понимать объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников. Рассматривая информацию с точки зрения отображения ее на каких-то или в каких-то материальных (физических) объектах, которые длительное время могут сохранять ее в отно-

[1]Шрейдер Ю.А. Об одной модели семантической теории информации // Проблемы кибернетики. Вып. 13. М., 1965.

сительно неизменном виде или переносить из одного места в другое, носителей защищаемой информации можно классифицировать следующим об разом:

– материально-вещественные носители (документы, книги, изделия, вещества и материалы);

– излучения и поля (электромагнитные, тепловые, радиационные и другие излучения, гидроакустические, сейсмические и другие поля);

– человек.

Колесников А.А.,
студент института информационных
технологий и безопасности
КубГТУ

Применение открытых источников персональных данных при проведении оперативно-розыскных мероприятий

Повышение эффективности работы правоохранительных органов по раскрытию и расследованию преступлений в сфере высоких технологий в настоящее время невозможно без интеграции в криминалистику новых информационных технологий.

В связи с совершенствованием технологий записи и хранения данных на людей обрушились колоссальные потоки информационной руды в самых различных областях. Деятельность любого предприятия (коммерческого, производственного, медицинского, научного и т.д.) теперь сопровождается регистрацией и записью всех подробностей его деятельности. Что делать с этой информацией? Стало ясно, что без продуктивной переработки потоки сырых данных образуют никому не нужную свалку.

Ученые давно признают потенциал Интернета для глубокого исследования сетей – потенциал, который во многом остается невостребованным.

Учитывая, что основным местом преступления является Интернет (или с использованием Интернета), то процесс сбора оперативной информации легко автоматизировать путем использования специальных программ, называемых интеллектуальными агентами (в среде программистов еще называемы «пауками»). Они способны проводить анализ сайтов, проводить целевой поиск информации в Интернет и тем самым находить потенциальных преступников.Специфика современных требований к такой переработке следующие:

- данные имеют неограниченный объем;
- данные являются разнородными (количественными, качественными, текстовыми);
- результаты должны быть конкретны и понятны;
- инструменты для обработки сырых данных должны быть просты в использовании.

Для наиболее удобного представления информации для дальнейшего ее анализа на сегодняшний день существует набор методов, который описывается термином - Datamining, что в переводе означает «Анализ данных». На сегодняшний день это очень прогрессивно развивающееся направление, которое нашло отражение в различных программных продуктах, которые используются для сбора, структуризации и анализа данных об каком – либо изучаемом предмете или человеке. Главная цель всех методов «Анализа данных» это представление информации в таком виде, при котором анализ данных превращается в тривиальную задачу.

Data Mining - это процесс обнаружения в сырых данных:

- ранее неизвестных;
- нетривиальных;
- практически полезных;
- и доступных интерпретации знаний;
- необходимых для принятия решений в различных сферах человеческой деятельности.

Визуализация социальной сети - метод представления структуры социальной сети в виде оптического изображения (например, в виде рисунков и фотографий, графиков, диаграмм, структурных схем, таблиц, карт и т. д.).

На текущий момент на рынке программного обеспечения представлен ряд инструментов для сбора и ввода данных, построения социограмм сетей и их статистического анализа. Перечисленные программные решения, как правило, имеют ориентацию на определенные исследовательские задачи.
При проведении анализа из большого перечня программных продуктов были исследованы следующие:

– Pajek;
– Maltego;
– Spoiltego.

Так как проблема очень обширна, поэтому в рамках исследования ограничимся только этими тремя программными продуктами. Приведем их характеристики.

Pajek – программных комплекс, который предназначен для визуального представления очень больших сетей в виде графов. При использовании данного программного продукта предполагается, что моделируемая сеть уже представлена в удобной для компьютера форме, а именно, в виде структурированного файла с разметкой языка NetML. На рис. 2 представлен пример работы программного комплекса.

Специфическими возможностями программы Pajek является ее ориентация на анализ и визуализацию больших социальных сетей, состоящих из миллионов узлов

Maltego - в отличии от предыдущего программного комплекса данный инструмент позволяет производить и сбор информации. Сбор необходимой информации осуществляется посредством так называемых «трансформеров». Трансформер - это всего лишь небольшая программа, которая способна предоставить информацию для анализа, проведя некоторый предварительный объем действий. На рисунке 3 представлен пример работы данной программы.

Spoiltego – программа, которая является видоизмененной версией Maltego. В отличии от Maltego этот программный продукт использует для сбора данных непосредственно локальные программы, написанные пользователем. Maltego же, в свою очередь ориентирована на работу с интернетом и с сервисами, кото-

рые предоставляет компания-разработчик. Внешний вид программы аналогичен Maltego.

Анализ программных продуктов показал, что на сегодняшний день существует множество программных продуктов, которые способны помочь в проведении оперативно-розыскных мероприятий в информационных системах, однако данные программные продукты созданы для анализа иностранных сервисов. Для реалий России такой набор является неполным, так как большая часть населения посещает такие социальные сети как «Вконтакте.ru» и "Одноклассники.ru".

В связи с этим исследователи поставили перед собой следующие задачи:

1. исследовать работу программы Maltego;
2. адаптировать выбранный программный продукт для поиска информации в российских социальных сетях.

Результатом исследования данной исследовательской работы явилось создание «Трансформера» для программы Maltego, который способен извлекать из страницы пользователя социальной сети «Одноклассники.ru» фотографию на аватаре и полный список id-номеров друзей пользователя. Выберем для произведения извлечения фотографии случайную страницу Одноклассников.

Если скопировать данную ссылку и открыть в браузере, то мы увидим картинку с главной страницы пользователя социальной сети.

Данный «Трансформер» является доказательством того, что для поиска информации в социальных сетях и подобных интернет-сервисах вовсе не обязательно создавать новые системы, достаточно просто модернизировать имеющиеся.

Аналогично можно написать так же «Трансформеры», которые будут вести поиск общих друзей, список групп и т.д. Полученная информация станет неоценимо полезной для оперативно-розыскных мероприятий. Еще больший плюс данного метода поиска информации в том, что производится поиск из открытых источников, что не противозаконно.

В рамках исследования был так же разработан «Трансформер», который считывает всех друзей пользователя социальной сети «Одноклассники.ru». На рис. 8 представлен результат работы «Трансформера», на рисунке расположено только 12 узлов на один запрос.

Не сложно видеть, что рассматриваемые пользователи социальной сети имеют общего друга, но так же возможно представить эти связи в другом виде.

Причем, в центре кругов находятся исследуемые профили людей, а по линии круга выставлены полученные друзья, общие вершины являются соединяющими для двух кругов.

Как видно из преведенных примеров, программа Maltego может стать очень полезным инструментом в проведении поиска связей между людьми.

Результатом данного исследования явилось получение мощного инструмента, позволяющего автоматизированно получать, обрабатывать и представлять информацию в удобном для анализа виде. Были изучены современные методы программирования,которые позволили создать агентов (Трансормеров) для поиска информации в сети Интернет.

Полученные результаты могут стать отправной точкой для написания пакета «Трансформеров», способных получать полную ифнормацию о пользователе, зарегистрированном в любой социальной сети России.

Луговенко Т.С.,
слушатель 4 курса 142 взвода
Краснодарского университета МВД России
Научный руководитель:
Стукалов В.В.,
кандидат юридических наук,
доцент кафедры ОРД в ОВД
Краснодарского университета МВД России

Организация взаимодействия следователя и оперативных подразделений

С точки зрения науки философии взаимодействие – философская категория, отражающая процессы воздействия объектов друг на друга, их взаимную обусловленность и порождение одним объектом другого. Взаимодействие – объективная и универ-

сальная форма движения, развития, определяет существование и структурную организацию любой материальной системы[1]. Переходя на более низкий уровень можно рассматривать конкретно взаимодействие органов внутренних дел так, как это делает наука ОРД: Взаимодействие – деятельность, заключающаяся в наиболее целесообразном выборе и реализации организационных и тактических мер, направленных на создание оптимальных условий для решения задач борьбы с преступностью путем осуществления упорядоченных и взаимоувязанных действий двух или более субъектов. Еще более конкретизируя понятие и оставаясь в рамках науки ОРД можно вывести что: Взаимодействие органов дознания и предварительного следствия это основанная на законе, согласованная по целям, месту и времени, деятельность данных субъектов, осуществляемая в целях предупреждения, раскрытия и расследования преступлений, а также розыска преступников.

Прежде всего, обращает на себя внимание конкретность принципов осуществления взаимодействия, что и не удивительно, поскольку непосредственно закон, как регулятор практической деятельности ОВД должен быть более конкретен, нежели общетеоретические научные выкладки[2]. Кроме принципов закон определяет основные задачи взаимодействия:

обеспечение неотложных следственных действий и оперативно– розыскных мероприятий при совершении преступлений;

всестороннее и объективное расследование преступлений, своевременное изобличение и привлечение к уголовной ответственности лиц, их совершивших, а также розыск скрывшихся преступников;

осуществление мероприятий, направленных на возмещение материального ущерба, причиненного гражданам и организациям вне зависимости от форм собственности преступными действиями виновных лиц[3].

---

[1]Энциклопедический словарь. Издание 2.– М., 2003г.

[2]Кулагин Н.И. Взаимодействие органов расследования с учреждениями массовой информации : учеб. пособие / Н.И. Кулагин, В.Н. Ростов. – Волгоград: Волгоград. Акад. МВД России, 2004. – С. 12.

[3]Кругликов А.П. Взаимодействие следователей и органов дознания по Уставу уголовного судопроизводства 1864 года // Российский следователь. – № 1. – 2005. – С. 54.

Хотелось бы отметить что если две первые задачи решаются в настоящее время органами внутренних дел на достаточно высоком уровне, то третья задача, а конкретнее возмещение материального ущерба в современных условиях является почти недостижимой. Юридическая наука выделяет также формы такого взаимодействия:

1. Обмен информацией
2. Совместное планирование
3. Совместный анализ и оценка оперативной обстановки
4. Совместная учеба и разбор реализованных дел
5. Совместная работа на месте происшествия.

Данные формы выведенные наукой нашли свое отражение в нормативной базе деятельности ОВД практически без изменений, а в завершение общей характеристики взаимодействия дознания и предварительного расследования хотелось бы привести нормативно-правовую основу данного взаимодействия:

Конституция Российской Федерации;

уголовное и уголовно-процессуальное законодательство Российской Федерации;

законодательство в сфере оперативно-розыскной деятельности;

международные договоры РФ по вопросам взаимодействия правоохранительных органов в сфере борьбы с преступностью;

Инструкция по организации взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений, ведомственные и межведомственные нормативные акты.

Таким образом, взаимодействие следователя и оперативных сотрудников в составе следственно–оперативной группы является одним из важнейших условий для успешного расследования и раскрытия преступлений. Оно строится на принципах законности, организующей роли следователя в проведении расследования, самостоятельности оперативных сотрудников в выборе средств и методов оперативно-розыскной деятельности, плановости и непрерывности и происходит в двух основных формах: процессуальной и организационной. Взаимодействие обеспечивает наиболее эффективную, организованную и плодотворную работу следователя и оперативных сотрудников, позволяет эко-

номить «драгоценные» силы, средства и время правоохранительных органов.

В соответствии с внутриведомственными нормативными актами взаимодействие между следователем, оперативным работником и дежурной частью начинается, как правило, с момента поступления в дежурную часть сообщения о преступлении, подследственном следователю. В органах внутренних дел сложилась четкая система дежурных частей, деятельность которых регламентируется ведомственными нормативными актами.

Дежурная часть обязана при поступлении сообщения о совершении или готовящемся преступлении немедленно на него реагировать, организовывать на этой стадии четкое взаимодействие следователя, оперативных работников, эксперта-криминалиста и других специалистов и их незамедлительный выезд для осмотра места происшествия, раскрытия преступления по горячим следам и задержании преступника[1].

Следовательно, своевременность и обоснованность возбуждения уголовного дела зависят от проверки обстоятельств происшествия, которые предшествует вынесению постановления о возбуждении уголовного дела. Таким образом, установление оснований возбуждения уголовного дела можно назвать предварительной проверкой повода к этому, будь то заявление гражданина или непосредственное обнаружение признаков преступления.

При этом одной из предпосылок успешного раскрытия преступления по горячим следам после получении сообщения о нем является быстрая и четкая организация выезда следственно-оперативной группы для осмотра места происшествия и принятия всех необходимых мер для задержания преступника.

Практика показывает, что при расследовании преступлений приходится проводить огромный объем работы следственно-оперативного характера. Результаты обмена информацией позволяют сформировать методическую и логическую схему оперативно-розыскных мероприятий и следственных действий, внести

[1]Бердичевский Ф.Ю. Взаимодействие органов следствия и дознания как организационная система // Советское государство и право - 1973. - № 12. -~ С. 106.

необходимые коррективы, наметить характер действий, связанных с использованием помощи специалистов требуемого профиля[1].

Но как показывает практика, взаимодействие следователя с оперативными подразделениями является слабым звеном в организации расследования преступлений. Специалисты отмечают, что нередко именно из-за слабой организации взаимодействия остаются нераскрытыми многие совершаемые преступления[2]. В частности, пока несовершенна система взаимного обмена информацией, наблюдается несогласованность при производстве следственных действий и оперативно-розыскных мероприятий. Следователи нерешительно, с неоправданным недоверием относятся к оперативно-розыскной информации при планировании и производстве расследования, а оперативные сотрудники не всегда своевременно и качественно выполняют их поручения о производстве розыскных и отдельных следственных действий по уголовным делам. Указанные недостатки в деятельности следственного аппарата в значительной мере являются результатом упущений в организации его работы.

В настоящее время в отечественной практике широко распространились основанные на специализации, постоянно действующие следственно-оперативные формирования по раскрытию и расследованию отдельных видов преступлений[3]. Поскольку данная форма организации работы имеет ряд преимуществ, на наш взгляд, этот подход наиболее оправдан в деятельности по раскрытию и расследованию преступлений, совершаемых в условиях неочевидности.

Представляется, что в УПК РФ необходимо предусмотреть возможность создания не только следственных групп (ст. 163 УПК РФ), но и следственно-оперативных групп, наделив, тем самым, последние процессуальными полномочиями на производ-

---

[1]Гусев А.В., Организационно-правовые проблемы взаимодействия следователя слицом, обладающим специальными знаниями / А.В. Гусев, С.А. Данильян // ЮристъПравоведъ. - 2011. - № 3. - С. 34-38.

[2]Косимов О.А.Проблемы взаимодействия следователя сорганами дознания на стадии возбуждения уголовного дела по материалам оперативно-розыскной деятельности / О.А.Косимов // Российский следователь. - 2011. - № 12. - С. 31.

[3]Кругликов А.П. Следственная и следственно-оперативная группы: проблемы взаимодействия следователей и органов дознания при их функционировании / А.П. Кругликов // Уголовное право. - 2010. - № 6. - С. 77.

ство предварительного следствия. В связи с этим в ст. 163 УПК РФ целесообразно установить, что руководитель следственного органа вправе принять решение о создании следственно-оперативной группы, о чем необходимо указать в постановлении о возбуждении уголовного дела или в постановлении о производстве предварительного следствия следственно-оперативной группой с указанием состава группы и о назначении руководителя, который принимает дело к своему производству.

Ляшенко В.С.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Противодействие несанкционированному доступу к источникам информации

Несанкционированный доступ (НСД) – получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

НСД может привести к утечке информации. Сразу можно увидеть и причины НСД к информации.

1. ошибки конфигурации
2. слабая защищенность средств авторизации
3. ошибки в программном обеспечении
4. злоупотребление служебными полномочиями
5. прослушивание
6. использование вредоносных программ на компьютерах сотрудников.

Последствия осуществления НСД к информации могут быть различными, в качестве примера можно привести:

- утечку персональных данных (сотрудников организации);

- утечку коммерческой тайны;
- утечку переписки;
- утечку государственной тайны;
- полное либо частичное лишение работоспособности системы безопасности.

Защита компьютеров от НСД является одной из основных проблем защиты информации, поэтому чаще всего заранее встраивают различные подсистемы защиты от НСД. Однако для серьезной защиты этого будет мало, и поэтому в дополнение к обычным программам защиты необходимо использовать специальные средства ограничения.

Любая система безопасности информации должна обеспечивать конфиденциальность, доступность и целостность информации. Таким образом, исходя из данных свойств, можно выделить 3 основных вида угроз: нарушения конфиденциальности, нарушения доступности, нарушения целостности. Эти угрозы являются первичными. К вторичным же угрозам обычно относят угрозу раскрытия параметров системы, которая предполагает знание злоумышленниками секретной информации: паролей, ключей, шифров, типов носителей информации и их расположения, технических характеристик объектов системы.

Средства защиты от НСД позволяют защищать информацию, хранимой и обрабатываемой на рабочих станциях и серверах, расположенных в локальных и территориально распределенных сетях. Данные средства можно разделить на две группы: средства ограничения физического доступа; средства защиты от НСД по сети.

Средства ограничения физического доступа или так называемые «электронные замки» являются наиболее надежным решением проблем ограничения физического доступа к рабочей станции и срабатывают до загрузки операционной системы. При входе запрашивается носитель с ключевой информацией, необходимой для его аутентификации. Если информация не предоставляется или пользователь не является пользователем защищаемой рабочей станции, такое средство блокирует загрузку операционной системы. Если аутентификация пользователя прошла успешно, но при загрузке была нарушена целостность хотя бы одного

файла из списка контролируемых, загрузка блокируется. При успешном прохождении всех проверок замок возвращает управление рабочей станции для загрузки штатной операционной системы.

Наиболее надежными средствами защиты от НСД по сети являются виртуальные частные сети и межсетевое экранирование.

В целом основными характеристиками средств защиты от НСД являются:

степень полноты охвата и качества системы разграничения доступа;

состав и качество обеспечивающих средств системы разграничения доступа;

гарантии и правильность функционирования системы разграничения доступа и обеспечивающих ее средств.

оперативная замена вышедших из строя технических средств.

В заключении можно сказать, что эффективность защиты информации достигается не количеством средств, потраченных на ее организацию, а способностью правильно реагировать на несанкционированный доступ к информации. Мероприятия по защите информации от несанкционированного доступа должны носить совокупный характер, т.е. объединять несхожие меры противодействия угрозам (правовые, организационные, программно-технические). Также следует учитывать и человеческий фактор и помнить, что основная угроза информационной безопасности компьютерных систем в большом количестве случаев исходит от самих сотрудников.

Магомедов И.Д.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Классификация персональных данных в кадровых подразделениях ОВД

Эффективность функционирования любой организации, включая органы внутренних дел, зависит от качества управления ее основными ресурсами. Среди них одно из главных мест занимает персонал. В первую очередь нужно определить, что относится к *персональным данным*. Это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)[1].

В Федеральном законе № 152 «О персональных данных», выделяются следующие виды персональных данных:

1. Общедоступные.

Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных. Так же, для защиты своих персональных данных в п.2 ст. 8 N 152-ФЗ «О персональных данных» закреплено положение о том, что сведения о субъекте персональных данных

[1]Ст3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ»О персональных данных»

могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

2. Биометрические.

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. Но в данном законе перечислены случаи, когда обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных. В связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, законодательством Российской Федерации об оперативно-розыскной деятельности, законодательством Российской Федерации о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию[1].

3. Обезличенные.

Персональные данные, в которых невозможно определить их принадлежность конкретному субъекту персональных данных. В ФЗ «О персональных данных» понятия «обезличенные персональные данные» в явном виде нет. В чистом виде обезличенные персональные данные обычно используются для решения статистических задач. Кроме того путем обезличивания можно снизить класс информационной системы персональных данных и, соответственно, затраты на ее защиту. К примеру, в информационной системе имеется база данных, в которой содержатся фамилия, имя, отчество, дата рождения и адрес человека. Если изъять из базы, скажем, адрес (т.е обезличить персональные данные), то без дополнительной информации (адреса) нарушитель не сможет однозначно определить субъекта персональных данных. В результате процесса изъятия адреса в данном примере персональные данные становятся обезличенными.

[1]Ст.11 Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»

4. Специальные категории.

Перечень специальных категорий персональных данных приведен в статье 10 Федерального закона «О персональных данных». К ним относят данные, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. В рамках Закона «О персональных данных» устанавливаются ограничения на основании обработки: это письменное согласие, законное основание или общедоступные персональные данные.

При обработке персональных данных в информационной системе может возникнуть угроза их безопасности. Под актуальными угрозами безопасности понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. Поэтому при обработке персональных данных в информационных системах устанавливаются уровни защищенности персональных данных, перечень которых дан в Постановлении правительства от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Контроль над выполнением требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом)[1].

Кадровая информация в ОВД существует в большом количестве учетных документов, сведения в которых дублируются.

[1]Постановление от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Это усложняет создание электронного хранилища данных о персонале, т.к. электронное личное дело сотрудника становится конгломератом разных документов. Поэтому необходима грамотная классификация персональных данных, необходима унификация и стандартизация документов персонального учета и порядка работы с ними в органах разных видов государственной службы, в том числе правоохранительной, приведение документов к оптимальному единообразию по составу и формам.

Мартынов Д.В.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Экспериментальное обоснование возможностей средств фото-, и видеоаппаратуры для добывания документированной информации

Документы представляют определенную ценность для разведок противника и относятся к наиболее информативным источникам, так как содержат, как правило, достоверную информацию в отработанном и сжатом виде, в особенности если документы подписаны или утверждены.

Сведения, содержащиеся в документах, могут добываться по визуально-оптическому с использованием различных технических средств наблюдения и фиксации визуальной информации. Для того, чтобы предпринять адекватные меры по защите информации от утечки по визуально-оптическому каналу, необходимо оценить возможности технических средств разведки. Вероятность обнаружения и распознавания объектов наблюдения характеризует риск утечки информации по оптическому каналу. На риск утечки информации по оптическим каналам утечки информации влияет, прежде всего, количество и точность измерения

видовых демаскирующих признаков объектов наблюдения, передаваемых по этим каналам. В свою очередь количество признаков и точность их измерения зависят от количества пикселей изображения объекта на сетчатке глаза, фотопленке или ПЗС-матрицы оптического приемника. Вероятность обнаружения и распознавания объектов наблюдения в видимом диапазоне света зависит, прежде всего, от количества пикселей изображения[1].

Количество пикселей, содержащееся в изображении объекта наблюдения, можно оценить по формуле линзы, иллюстрируемой рис. 1.

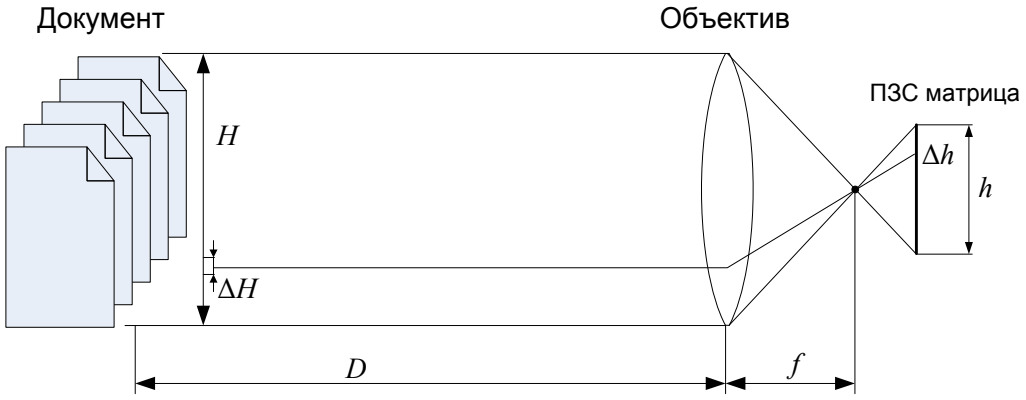


Рис. 1 Схема наблюдения объекта

На рисунке объект высотой H создает изображение высотой h. Точка изображения размером Δh соответствует элементу объекта размером ΔH. Для объекта, расположенного на удалении D от объектива, средства наблюдения выполняется равенство[2]:

$$\Delta h = \frac{\Delta H \mathrm{f}}{D}.$$

Количество пикселей, укладывающихся в размер Δh, равно ΔhR, где R — разрешающая способность средства наблюдения в пик/мм.

Окончательно, количество пикселей N в Δh определяется как

$$N = \frac{R \Delta H \mathrm{f}}{D}.$$

---

[1]Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности — М.: Гелиос АРВ, 2005. — 960 с

[2]Гарсия М. Проектирование и оценка систем физической защиты информации. Пер с англ. – М.: Мир: ООО «Издательство АСТ», 2002 – 368 с.

Рассчитаем расстояние, при съемке с которого невозможно будет распознать текст. Вероятность распознавания формы объекта без помех по его изображению, образуемому из более чем 7-8 точек по горизонтали и вертикали, приближается к 1. Безошибочно распознаются цифры и буквы текста, напечатанного 9 игольчатым принтером. По усредненным данным минимальное количество точек изображения, обеспечивающее вероятность 0,9 обнаружения (распознавания) объекта простой формы, образуют матрицу из (5-6)х(5-6)точек[1].

Для размера прописной буквы примем N=5, при котором практически невозможно распознать текст, написанный как прописными, так и строчными буквами.

Таким образом, максимальное расстояние, с которого возможно получение документированной информации равно:

$$D = \frac{R\Delta H\mathrm{f}}{5}.$$

Параметр ΔH получен экспериментальным путем и для основных размеров шрифта TimesNewRoman приведен в табл. 1.

Таблица 1 – Высота букв для различного размера шрифта

Шрифт	ΔH, мм	
	строчные	Прописные
TimesNewRoman 10	1,55	2,3
TimesNewRoman 11	1,7	2,55
Times New Roman 12	1,9	2,8
Times New Roman 14	2,2	3,3
Times New Roman 16	2,5	3,7

Определим значение разрешения по вертикали. Из технической документации любого фотоаппарата или видеокамеры известна диагональ ПЗС матрицы Д, соотношение сторон В/Ш, количество эффективных пикселей K_n.

[1]Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности — М.: Гелиос АРВ, 2005. — 960 с

Разрешение по вертикали, т.е. количество пикселей на единицу длины (мм) находится как отношение количества пикселей по вертикали к размеру в мм ПЗС матрицы:

$$R = \frac{K_{ïê}}{P_â}.$$

Определить количество точек по вертикали можно по формуле:

$$K_{пв} = \sqrt{\frac{K_п \cdot В}{Ш}}.$$

Размер, в мм по вертикали вычисляется по формуле:

$$P_в = \frac{Д \cdot В}{\sqrt{В^2 + Ш^2}}.$$

Для соотношения В/Ш=3/4, формулу можно упростить:

$$P_в = 0{,}6Д$$

Пример расчета для фотоаппарата CanonPowerShotA 1100.

Из инструкции по эксплуатации нам необходимы следующие характеристики:

Диагональ ПЗС матрицы $Ä = 1/2{,}3'' \approx 11\ ìì$.

Соотношение сторон В/Ш=3/4.

Количество эффективных пикселей $K_ï = 12{,}1$ млн.

Максимальное фокусное расстояние: f=24,8 мм.

$$K_{пв} = \sqrt{\frac{12{,}1 \cdot 10^6 \cdot 3}{4}} = 3013 \text{ пик.}$$

$$P_в = \frac{11 \cdot 3}{5} = 6{,}6 \text{ мм}$$

$$R = \frac{3013}{6{,}6} = 457 \text{ пик/мм}$$

Для текста, написанного шрифтом TimesNewRoman 14, максимальное расстояние наблюдения будет равно:

$$D = \frac{457 \cdot 3{,}3 \cdot 24{,}8}{5} \approx 7{,}5 \text{ м}$$

Полученные расчетные значения были проверены практически, путем фотографирования листа с текстом с различных расстояний.

Малкондуев А.М.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Технические каналы утечки информации

Владение информацией во все времена давало преимущества той стороне, которая располагала более точной и обширной информацией, тем более, если это касалось информации о своих соперниках.

В связи с научно-техническим прогрессом и быстрым ростом развития общества наиболее распространенным ресурсом является информация, а следовательно её ценность и охрана является очень важным элементом. «Кто владеет информацией, тот владеет миром». В этом, несомненно, есть суть, которая выражает нынешнюю сложившуюся в мире ситуацию. Так как разглашение определенной ситуации может привести к негативным последствиям для её владельца, её защита от несанкционированного доступа стала проблемной.

Утечка информации — это ее бесконтрольный выход за пределы организации (территории, здания, помещения) или круга лиц, которым она была доверена.

Защитить информацию значит:

- обеспечить физическую целостность информации, т.е. не допустить искажений или уничтожения элементов информации;
- не допустить подмены элементов информации при сохранении её целостности;
- не допустить не санкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;
- быть уверенным в том, что передаваемые владельцем информации ресурсы будут использоваться только в соответствии с обговоренными сторонами условиями.

Чтоб возник канал утечки информации необходимы определенные условия, такие как: пространственные, временные, энергетические, а так же средства восприятия и фиксации информации. Поскольку на каждую защиту находится способ ее преодоления, то для обеспечения должной защищенности информации необходимо постоянно совершенствовать методы.

В виду сложившейся обстановки принято выделять ряд выводов:

1.Безопасных технических средств нет.

2. Источниками образования технических каналов утечки информации являются физические преобразования.

3. Любой электронный элемент при определенных условиях может стать источником образования канала утечки информации.

4. Любой канал утечки информации может быть обнаружен и локализован.

5. Канал утечки информации легче локализовать, чем обнаружить.

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

– визуально-оптические;

– акустические (включая и акустико-преобразовательные);

– электромагнитные (включая магнитные и электрические);

– материально-вещественные (бумага, фото, магнитные носители).

Визуально-оптические каналы — это, как правило, непосредственное или удаленное наблюдение.

Переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах. Предупреждение утечки информации по акустическим каналам сводится к пассивным и активным способам защиты. Соответственно, все приспособления защиты информации можно смело разделить на два больших класса – пассивные и активные. Пассивные – измеряют, определяют, локализуют каналы утечки, ничего не внося при этом во внешнюю среду. Активные – «зашумляют», «выжигают», «раскачивают» и уничтожают всевозможные спецсредства негласного получения информации.

В акустическом канале переносчиком информации выступает звук, лежащий в полосе ультра слышимого (более 20 000 Гц) и инфразвукового диапазонов. Диапазон звуковых частот, слышимых человеком, лежит в пределах от 16 до 20 000 Гц, и содержащихся в человеческой речи — от 100 до 6000 Гц.

Переносчиком информации являются *электромагнитные волны* в диапазоне от сверхдлинных с длиной волны 10 000 м (частоты менее 30 Гц) до субмиллиметровых с длиной волны 1 - 0,1 мм (частоты от 300 до 3000 ГГц).

Материально-вещественными каналами утечки информации выступают самые различные материала в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства, бракованные изделия, черновые материалы и другое.

Для выявления утечки информации необходим системный контроль
возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения).

Локализовать канал утечки информации можно при помощи организационных, организационно-технических и технических мер и средств.

В заключение следует отметить, что при защите информации от утечки по любому из рассмотренных каналов следует придерживаться следующего порядка действий:

1) Выявление возможных каналов утечки.

2) Обнаружение реальных каналов.

3) Оценка опасности реальных каналов.

4) Локализация опасных каналов утечки информации.

5) Систематический контроль за наличием каналов и качеством их защиты.

Мамедов Э.М.,
курсант 5 курса
Краснодарского университета МВД России
Научный руководитель:
Запорожец Е.В.,
преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России

Развитие течения ваххабизма как религиозного терроризма на Северном Кавказе

Северный Кавказ представляет собой специфический регион, где сошлись ведущие мировые религии (христианство, ислам, буддизм), стороны света (Запад и Восток, Север и Юг), континенты (Европа и Азия). Здесь соприкасаются многие народы, культуры, конфессии, проживает множество народов и этнонациональных групп, имеющих друг к другу немало претензий территориального и иного характера. Можно сказать, что Северный Кавказ обладает своим особым обликом, своими специфическими особенностями, отличающими его от всех других регионов.

Религия, будучи специфической подсистемой общества, многообразными связями переплетена с другими компонентами общественной системы. Она является существенным и постоянно действующим фактором общественной жизни и проявляется посредством выполнения определенных социальных функций, через деятельность религиозных институтов, организаций, верующих масс. Для религий характерны как этносегрегирующая функция, ведущая к противопоставлению народов и последователей разных вероисповеданий, так и интегративная и регулятивная функции, которые позволяют устанавливать связи между единоверцами, поддерживать конфессиональную и этническую общность, регулировать поведение людней. Эти функции на протяжении веков использовались для обеспечения целостности общества, ослабления существующих противоречий, улаживания межэтнических и других конфликтов.

С точки зрения некоторых этнографов, ваххабиты – сравнительно новое течение, вызванное обострением социально-

экономических и политических условий между частью бедуинского населения, а также части религиозных деятелей, выразившееся как протест против богатства городских жителей и богачей. Также движение сыграло значительную роль в освободительной войне против Турции.

Обычно люди употребляют слово «ваххабит» против каждого, кто противоречит их обычаям, убеждениям и религиозным нововведениям, даже если эти убеждения являются порочными, противоречат Благородному Корану и достоверным хадисам. Особенно употребляется против призыва к единобожию и взыванию только к Аллаху, и никому более. Ваххабиты отвергают различные, с их точки зрения, нововведения, не дозволенные исламом.

В 1980-е годы среди советских мусульман стали распространяться идеи исламского фундаментализма. Сторонники «чистого ислама», как они себя называли, заметно выделялись из основной массы верующих активным неприятием «безбожного» общества, оппозицией к «официальному» мусульманскому духовенству и критическим отношением к «народному исламу». За ними прочно закрепилось наименование «ваххабитов», хотя они таковыми себя не считали.

В 1990-е годы Северный Кавказ стал тем регионом России, где конфронтация между сторонниками «чистого» и «традиционного» ислама стала наиболее острой.

По мнению Р.А. Силантьева: «Сейчас под ваххабизмом понимается не конкретная и чётко выраженная религиозная идея, а совокупность идеологий исламского происхождения, проповедующих крайнюю нетерпимость к инаковерующим и инакомыслящим. И оправдывающих их убийство. Проще говоря, традиционные мусульмане уживаются с представителями иных исповеданий, а ваххабиты – нет».

Висхан Халидов отмечает, что «центральное место в идейной платформе сторонников ваххабизма занимает концепция непризнания любой власти, отходящей от предписаний шариата».

По некоторым оценкам, количество ваххабитов в России на настоящее время составляет около 700 тысяч человек.

В начале 1990-х в Дагестане обострились отношения между приверженцами традиционного для данного региона суфизма и

«ваххабитами». Лидером дагестанских ваххабитов долгое время считался Багаутдин Кебедов. На 16 сентября1999 года ваххабитской территорией считалась Кадарская зона. Народным Собранием Республики Дагестан был принят Закон «О запрете ваххабитской и иной экстремистской деятельности на территории Республики Дагестан», а в 1999 многие ваххабиты приняли участие во вторжении боевиков из Чечни в Дагестан.

Согласно социологическому исследованию, проведенному в 2004 году Дагестанским центром РАН, 83% служителей исламского культа и до 40% верующих в республике придерживались фундаменталистских взглядов [5].

В межвоенной Чечне центром «ваххабизма» считался Урус-Мартан, в котором находился джамаат Рамзана Ахмадова. В 1998 в Гудермесе произошло вооруженное столкновение между бойцами Арби Бараева и членами «Национальной гвардии» Сулима Ямадаева. 25 июля1998 года по инициативе муфтия Ахмада Кадырова в Грозном прошёл съезд членов ДУМов из разных регионов Кавказа, на котором прозвучало осуждение ваххабизма, указом президента республики ваххабизм был объявлен вне закона, несколько ваххабитских миссионеров-иорданцев выдворено из Чечни.

Безопасность и стабильность на Северном Кавказе во многих отношениях зависит от положения в соседних южных странах ближнего и дальнего зарубежья. С точки зрения региональной и национальной безопасности важнейшими факторами во внешнеполитической стратегии России являются закавказские государства, которые соединяют в качестве промежуточного звена в единую дугу нестабильности два остальных источника конфликтов в этом регионе: ближневосточный и северокавказский, Эта дуга нестабильности стала серьезным фактором в дезинтеграционных процессах, происходящих на южных рубежах России.

Следует отметить, что исламские теологи выражают несогласие с использованием понятия фундаментализм при характеристике радикальных течений в исламе, ибо идеологи фундаментализма, по собственному убеждению преследуют священную цель - возвращение к регулятивным нормам раннего классического ислама, причем в системе “политика - ислам” сакральное начало берет на себя роль источника человеческих законов, вы-

ражения духовных и политических ценностей, следовательно, понятия “экстремизм”, “терроризм” и др., не вписывающиеся в данный механизм, просто теряют смысл.

Употребление понятия “ваххабиты” в широком смысле слова представляется не совсем корректным, так как на Северном Кавказе ваххабитами называют все группы мусульман, выступающие с критикой региональных особенностей ислама, обычно дополняемого местными обычаями и светскими ритуалами. Как следствие, в ваххабиты зачисляют всех, исповедующих ислам и выступающих с критикой официального духовенства. Более правильно называть северокавказских ваххабитов салафитами (мусульманские религиозные деятели, которые в различные периоды истории выступали с призывами ориентироваться на образ жизни и веру ранней мусульманской общины) или как указано выше - фундаменталистами.

Исламские экстремисты при обосновании своей радикальной позиции исходят из формулы, что сопротивление несправедливости - обязанность мусульманина и игнорирование этой обязанности - грех. Высшая справедливость наступит в обществе лишь тогда, когда мусульмане будут строго следовать шариату и эта принципиальная позиция принесет людям благоденствие и процветание.

При реализации своих идеологических установок исламские экстремисты игнорируют существующие политические и социально-экономические условия жизни общества, считая их производными от ислама. По их мнению, лишь религиозные идеалы определяют весь спектр социальных взаимоотношений людей. Отсюда следует вывод: позитивное развитие общества возможно исключительно на основе законов шариата. Чтобы обеспечить торжество законов шариата, необходимо призывать и выводить людей из неисламского общества (джахилийи), что возможно лишь при условии, если движение возрождения общества возглавят «истинные мусульмане».

Под последними понимаются верующие в Аллаха, отказавшиеся от всех привязанностей, в том числе близких и родственников, не разделяющих их идеологических установок. По существу это фанатики, воспринимающие нераздельность политических и религиозных ориентиров, опирающиеся как в вере, так и в

реальной жизни на раннюю исламскую идеологию, стремящиеся к установлению на земле власти Аллаха на основе шариата, убежденные в необходимости джихада, позволяющего применять насилие до полной победы ислама. Религиозные экстремисты отличаются исключительной преданностью своим руководителям, готовы выполнить их любой приказ, в том числе пожертвовать собственной жизнью во имя религиозных идеалов, не говоря уже о жизни так называемых “неверных”.

Борьба с терроризмом на религиозной основе - сложнейшая, многоплановая и актуальная для Российской Федерации задача общегосударственного масштаба. Силовой вариант решения проблемы способен дать лишь кратковременные позитивные результаты. Для кардинального оздоровления ситуации нужна кропотливая и прицельная работа по выявлению и ликвидации факторов, детерминирующих терроризм на религиозной основе, а также той питательной среды, на которой он произрастает. Для уничтожения этого социального зла необходимо взаимодействие государственных институтов, общественных объединений, партий, исламских организаций и движений, средств массовой информации, всех законопослушных граждан.

Масорик А.О.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Средства связи ОВД

Эффективность охраны общественного порядка, проведения оперативных мероприятий по борьбе с преступностью во многом определяется качеством управления органами внутренних дел и их подразделениями.

Основным средством, обеспечивающим непрерывное управление силами и средствами ОВД и их подразделений, является связь. От ее умелой и своевременной организации зависит успех решения оперативных задач в условиях быстро меняющейся обстановки. Поэтому своевременная организация и поддержание надежной связи с подчиненными и взаимодействующими органами внутренних дел и их подразделениями являются важнейшей обязанностью начальника ОВД. Потеря связи может привести к частичной или полной потере управления. Перед связью ставятся две основные задачи:

1. Обеспечить начальнику ОВД возможность непрерывного оперативного управления подчиненными органами и подразделениями.

2. Обеспечить оперативную передачу вышестоящему начальнику, подчиненным и взаимодействующим органам внутренних дел и их подразделениям информации о готовящихся или совершенных преступлениях, о пожарах и стихийных бедствиях, а также сообщение им других сведений служебного характера. Для решения этих и других задач оперативного характера во всех органах внутренних дел создаются системы связи. Принципы построения системы:

- базовое звено
- узел связи;
- комплексное использование средств связи;
-обеспечение централизованного управления и взаимодействия;
- иерархичность системы, т.е. подсистема низкого уровня является составной частью системы более высокого уровня;
- соответствие требованиям единой технической политики министерства в части иерархии, структуры, взаимодействия (ведомственного и межведомственного) сетей связи, частотно-территориального планирования, номенклатуры и использования средств связи;
- согласованность с действующими нормативными и законодательными актами в области связи.

Построение системы связи ОВД определяется его структурой, местом нахождения и характером выполняемых задач. Система связи ОВД должна быть общей для всех служб и

подразделений. Она предполагает комплексное использование средств связи, обеспечение централизованного управления и взаимодействия в любых условиях оперативной обстановки. Комплексное использование средств связи достигается одновременным применением на одном направлении различных видов связи:

- радиосвязь (ВЧ радиосвязь, ОВЧ радиосвязь, радиорелейная связь и т.д.);
- проводная связь (низкочастотная и высокочастотная телефония, буквопечатающая телеграфия, факсимильная связь, системы прикладного телевидения);
- комбинированная связь (пейджинговая, транкинговая, сотовая, спутниковая).

Для обеспечения дежурным частям возможности централизованного управления силами и средствами ОВД, несущими патрульно-постовую службу, выполняющими оперативно-розыскные или иные мероприятия, организуются узлы оперативной связи. Они могут быть стационарными или передвижными.

Стационарные узлы размещаются в помещениях дежурных частей ОВД по месту их постоянного нахождения, а передвижные - оборудуются в различных пунктах на время, в течение которого необходимо обеспечивать связь из этого пункта.

К связи предъявляются ряд требований, важнейшими из которых являются:

- своевременность установления;
- надежность;
- пропускная способность;
- достоверность;
- скрытность.

Одним из основных средств связи, способным обеспечить непрерывное управление ОВД и их подразделениями в сложных условиях оперативной обстановки, является радиосвязь.

Важнейшим преимуществом радиосвязи по сравнению с другими средствами связи является ее высокая мобильность, позволяющая в минимальные сроки сконцентрировать в определенном месте необходимое количество сил и средств для проведения оперативно-розыскных мероприятий по розыску и

задержанию преступников, пресечению групповых хулиганств, ликвидации последствий пожаров и стихийных бедствий.

В работе подвижных групп при проведении оперативных мероприятий радиосвязь является единственным средством связи.

При организации радиосвязи необходимо учитывать ряд специфических факторов, влияющих на дальность и качество связи:

- характер и рельеф местности, экранирующее воздействие зданий, сооружений, линий электропередач;
- воздействие атмосферных и индустриальных радиопомех;
- уменьшение дальности действия радиостанций при работе в движении;
- возможность возникновения взаимных радиопомех от других радиотехнических средств, работающих в том же пункте. Кроме того, при организации радиосвязи необходимо учитывать возможность подслушивания переговоров.

Основными способами организации радиосвязи в ОВД являются радионаправления и радиосети.

Радионаправление – это способ организации радиосвязи между двумя корреспондентами, радиостанции которых работают на установленных только для них радиоданных, которые включают в себя порядковые номера радионаправлений, рабочие и запасные частоты, тип и мощность радиостанций, позывные, время работы.

Радиосеть – способ организации радиосвязи между несколькими (тремя и более) корреспондентами, которые работают на общих для них радиоданных.

Радиосвязь по направлениям обладает большей пропускной способностью и устойчивостью, чем по радиосетям. Однако, способ организации радиосетей имеет ряд преимуществ: он обеспечивает возможность ведения циркулярных передач и, что особенно важно, требует значительно меньшего количества радиостанций и частот. Поэтому ***основным способом организации радиосвязи в ОВД является создание радиосетей***. В каждой радиосети и в каждом радионаправлении указанием начальника ОВД назначается главная радиостанция, которая осуществляет контроль за соблюдением дисциплины связи и правильным использованием радиоданных. *Главная*

радиостанция регулирует порядок радиообмена, дает разрешение на установление связи между подчиненными радиостанциями.

В зависимости от характера решаемых оперативно-служебных задач радионаправления и радиосети могут быть постоянными или временными. *Постоянные радиосети* создаются при авто патрулировании, ведении надзора за движением транспорта и для связи ОВД между собой. *Временные радиосети* создаются при проведении разовых мероприятий.

По характеру обмена радиосвязь может быть симплексной, полудуплексной, дуплексной.

При *симплексном* радиообмене радиостанции передачу и прием ведут поочередно на одной частоте или на разных частотах приема и передачи (двухчастотный симплексный режим).

При *дуплексном* радиообмене радиостанции передачу и прием ведут одновременно.

При *полудуплексном* – передача и прием ведутся поочередно, но принимающая радиостанция имеет возможность приостановить работу передающей, не дожидаясь конца ее передачи. Полудуплексная связь характерна для диспетчерских сетей связи, где диспетчерская радиостанция работает в дуплексном режиме, а радиостанции остальных корреспондентов - в режиме двухчастотного симплекса.

Радиосвязь между радиостанциями ОВД осуществляется по единым для всех правилам. Эти правила определяют порядок установления радиосвязи, ее ведения и завершения. Кроме того, правила радиообмена определяют перечень сведений, разрешенных к передаче открытым текстом. Разрешено открыто передавать сведения:

- о правонарушениях (вид, место, время);
- об обнаружении трупа или лица, находящегося в беспомощном состоянии;
- о стихийных бедствиях и несчастных случаях (без указания количества человеческих жертв и причиненного ущерба);
- о вызове сил и средств для обеспечения охраны общественного порядка, предупреждения или пресечения преступления;
- о дорожно-транспортных происшествиях и пострадавших (без указания количества человеческих жертв);

- вызов медицинской помощи к месту происшествия;

- о прохождении спортивно-массовых и других подобных мероприятиях (без указания названия спортивных команд);

- о метеорологических, дорожных условиях;

- о пожарах и обстановке на них (без указания количества человеческих жертв), вызове сил для тушения.

Радиообмен должен быть четким и кратким. Переговоры по личным вопросам **запрещаются.** Вмешиваться в радиообмен между двумя радиостанциями и перебивать их работу разрешается только главным радиостанциям, а остальным радиостанциям - только при чрезвычайных обстоятельствах.

Радиосвязь в ВЧ-диапазоне осуществляется пространственной волной на расстояниях от 100 до 1000 и более километров. При организации связи в ВЧ-диапазоне пространственной волной на большие расстояния необходимо учитывать географическое направление линий радиосвязи, время суток, сезон года и протяженность линии радиосвязи, так как влияние этих факторов связано с состоянием и положением слоев ионосферы над земной поверхностью, что определяет выбор частот в этом диапазоне коротких волн, соответствующих данному месту и данному времени. ВЧ-связь применяется, главным образом, для связи радиостанций министерств, управлений и горрайорганов внутренних дел, дисло-цированных на расстояниях, превышающих технические возможности ОВЧ-радиостанций.

Применение этого вида радиосвязи может приводить к определенным неудобствам в практическом использовании из-за «капризов» ионосферы. Однако, обширные исследования, проведенные в последнее время в этой области радиосвязи, позволили создать Быстро адаптивные системы ВЧ-радиосвязи (FARCOS), которые отличаются высокой степенью гибкости и могут быть использованы для организации как стационарной, так и подвижной связи в ВЧ-диапазоне.

Радиорелейная связь (РРС) 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.

РРС основана на принципе ретрансляции (прием сигналов, их усиление и излучение к следующей станции), осуществляемой с помощью специальных антенн направленного действия (рупорные, параболические и др.).

Принцип действия радиорелейной линии (РРЛ) связи состоит в многократной ретрансляции радиосигналов промежуточными радио-станциями между двумя или более оконечными радиостанциями. Радиорелейные станции имеют специальные устройства многоканального уплотнения, что позволяет ретранслировать по РРЛ одновременно телефонные переговоры, телеграфные и даже телевизионные передачи. На РРЛ используется дуплексный способ связи.

Наумская Ю.Ю.,
студент института информационных
технологий и безопасности
Куб ГТУ

Кибертерроризм и мировое сообщество

Современное сообщество на прямую связанно с использованием информационно-коммуникационных и компьютерных технологий, и ежедневно в мире фиксируются множество попыток несанкционированного воздействия и доступа к банковским, военным и прочим компьютерным системам – компьютерные преступления.

На основе компьютерных преступлений формируется кибертерроризм. Понимая термин «терроризм» и сочетая его с представлением компьютерного (виртуального) пространства, можно вывести следующее определение: кибертерроризм – комплекс преднамеренных мер, направленных на информацию, обрабатываемую компьютером и компьютерными системами, представляющий собой опасность для жизни и здоровья людей, с целью нарушения общественной безопасности.

Понятия «киберпреступность» и «кибертерроризм» в каждой стране трактуются по своему, не имея единого определения.

Так же они не имеют определенной, разделяющих их грани, но для осуществления каждого необходимо использование компьютерных технологий. Ущерб от данных видов преступности может иметь как высокую государственную опасность (выведение из строя систем управления промышленных предприятий), так и не столь важную (электронные хищения, хищения денежных средств при помощи банковских карт).

Особое внимание борьба с кибертерроризмом получила после 2010 года, когда в Иранском Центре по обогащению урана был обнаружен вирус Stuxnet, выведший из строя ядерные центрифуги. До этого момента защита была направлена в основном на личную информацию, банковские данные. Теперь же вниманию развитых стран предоставляется безопасность объектов критической инфраструктуры: системы управления АЭС, плотин, промышленные предприятия, командные пункты ядерных сил.

Все ведущие мировые международные организации признают опасность киберпреступности, ее трансграничный характер и ограниченность подхода к решению этой проблемы. Признаются так же необходимость международного сотрудничества в выработке международного законодательства и принятии необходимых технических мер. Важную роль в борьбе с киберпреступностью и кибертерроризмом играют такие организации, как ОЭСР, Совет Европы, Европейский союз, ООН.

Первым на рассмотрение проблему киберпреступности и уголовно-правовых мер по борьбе с ней вывела Организация экономического сотрудничества и развития (ОЭСР), изучавшая с 1983 по 1985 гг. возможности гармонизации норм, предусматривающих уголовную ответственность за киберпреступления. Выводы были изложены в докладе «Преступления, связанные с компьютером: анализ правовой политики», в котором выведены результаты анализа существующего законодательства и сделаны предложения по его реформированию.

С 1985 по 1989 гг. Специальный комитет экспертов Совета Европы по вопросам преступности, связанной с компьютерами, выработал Рекомендацию № 89, утвержденную комитетом Министров ЕС 13.09.1989 г. Рекомендация содержит список правонарушений, рекомендованный странам-участницам ЕС для раз-

работки единой уголовной стратегии относительно компьютерных преступлений.

В 1995 году был опубликован «Справочник ООН по предотвращению и контролю преступности, связанной с компьютерами». В этом документе описывается и исследуется явления компьютерной преступности, описан анализ существующего уголовного права о защите данных и информации, рассматриваются вопросы предотвращения преступлений в киберпространстве и возможности международного сотрудничества в решении этих проблем.

В мае 2000 прошла конференция по кибепреступности, проведенная «Большой восьмеркой», главной темой была координация усилий по борьбе с преступностью в Интернете.

23 ноября 2001 года была в Будапеште принята Конвенция Совета Европы о киберпреступности – один из важнейших документов, регулирующий правоотношения в сфере глобальной компьютерной сети.

Кибербезопасность – одна из основных целей настоящего времени, которая требует постоянного совершенствования. Существует уже немало международных соглашений, норм, принципов, но они требуют еще некоторых доработок и, прежде всего, реализации.

Министр иностранных дел Великобритании Уильям Хейг на Лондонской конференции «Киберпространство» (1-2 ноября 2011г.) выдвинул в качестве основы для более эффективного сотрудничества между государствами, бизнесом и организациями семь принципов:

1. Необходимость действия правительства в сфере киберпространства соразмерено и в соответствии с международным правом:

2. Необходимость общего доступа к киберпространству, располагая необходимыми умениями, знанием технологий, уверенностью в своей безопасности;

3. Необходимость проявления толерантности среди пользователей киберпространства, уважение к языковым, культурным и идеологическим различиям;

4. Необходимость открытости киберпространства для инновационных процессов и свободного доступа идей, информации и самовыражения;

5. Необходимость уважения права на частную жизнь и предоставления защиты интеллектуальной собственности;

6. Необходимость коллективного сотрудничества по противодействию угрозе со стороны преступников, действующих онлайн;

7. Создание атмосферы конкуренции, которая обеспечит справедливые доходы от вложений в сети, услуг и содержания.

Немаловажным фактором в борьбе с кибертерроризмом может стать оперативный обмен информацией, который обеспечит взаимовыгодный обмен между правительствами и между региональными организациями. Антитеррористический центр СНГ и некоторые региональные организации (как РАТС ШОС) подписали соглашения, которые позволяют осуществлять обмен информацией. Так же в мае 2010 г. в Анталии страны СВМДА договорились обмениваться информацией в области правоохранительной деятельности и укрепления контактов между главами полицейских ведомств.

В 2012 г. Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам Секретариата ОБСЕ (ДПТУ/АТП) организовало четыре экспертных онлайн-форума с целью укрепления и дальнейшего стимулирования обмена информацией о последних тенденциях и спорах в отношении использования террористами Интернета, актуальных сложных вопросах, связанных с реагированием на такие угрозы, а так же применимой передовой практике и вариантах политики.

С развитием Интернета, распространение информации стало гораздо проще, быстрее и не требует больших затрат. Это, в свою очередь, стали использовать террористы в своих целях: распространяется террористическая пропаганда, поощряющая радикализацию и вербовку; террористы получают необходимую информацию; используется перевод денежных средств; связь между группами; подготовка и планирование терактов.

Так же как террористы используют Интеренет в своих целях, его можно использовать и против них. Предпринимаются меры обеспечения безопасности кибепространства целью предот-

вращения возможных негативных последствий использования Интернета в террористических целях. Но использование Интернета террористами может интерпретироваться как право на свободу высказывания, регулируемого соответствующими национальными законами.

В некоторых специальных службах и правоохранительных органах имеются специальные подразделения, работающие по вопросам киберпространства. А если рассматривать международный уровень, то можно привести в пример резолюцию по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности, изданную Генеральной Ассамблеи ООН.

Рабочая группа ЦГОКМ ООН по борьбе с использованием Интернета в террористических целях предприняла попытку составления перечня существующей практики, инструментов, таких как законы и конвенции, программы и ресурсы, призванных способствовать противодействию использования Интернета в террористических целях.

Одним из действенных способов привлечения к ответственности кибертеррористов является гармонизированная международная правовая система. Эта система позволяет не только привести законы к общему характеру, но и укрепить международное сотрудничество, так как необходимо регулярно пересматривать национальные правовые системы в соответствии с изменениями, чтобы учитывать быстрое развитие технологий.

В сентябре 2010 г. в Екатеринбурге на второй международной встрече высоких представителей, которые курируют вопросы безопасности, была представлена Конвенция об обеспечении международной информационной безопасности, разработанная Российской Федерацией. Предполагается, что эта концепция может послужить основой для выработки универсальной Конвенции под эгидой ООН.

Целью предлагаемой Конвенции является противодействие используемых информационных и коммуникационных технологий для нарушения международного мира и безопасности. В соответствии с положениями, государства-участники обязуются сотрудничать друг с другом в сфере обеспечения международной

информационной безопасности для поддержания мира и содействия международной экономической стабильности.

В Российской Федерации основные усилия направлены на совершенствование уголовной ответственности за совершение компьютерных преступлений, либо на изучение характеристики киберпреступности, но до сих пор не ведутся комплексные исследования по кибертерроризму и киберпреступности.

18 июня 2013 года на саммите «Большой восьмерки», проходившем в Лох-Эрне, президентами Российской Федерации и США было принято решение о создании двусторонней рабочей группы по вопросам угроз в сфере использования информационно-коммуникационных технологий в контексте международной безопасности. Лидеры двух стран отмечают, что угрозы в сфере использования ИКТ включают военно-политические и криминальные угрозы, а также угрозы террористического характера, в связи с чем относятся к наиболее серьезным проблемам национальной и международной безопасности.

15 января 2013 г. вступил в силу Указ Президента РФ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», в котором указаны основные задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, определены обязанности Федеральной службы безопасности РФ.

В итоге хотелось бы выделить основные причины, препятствующие созданию полноценной международной стратегии по борьбе с киберпреступностью и кибертерроризму:

Во-первых, до сих пор не был разработан полный и единый международный список кибепреступлений, отсутствует гармоничный сводок определений в данной сфере, законопроекты государств существенно различны;

Во-вторых, конечно же, непрерывное развитие киберпространства – территории совершаемых преступлений;

В-третьих, недостаток высококвалифицированных специалистов и экспертов, осведомленных в сфере кибербезопасности.

Нестеренко И.В.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Обеспечение конфиденциальности персональных данных путём их обезличивания

В соответствии с Федеральным законом от 20.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» под конфиденциальностью понимается обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Под персональными данными понимают любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Вступление в действие Федерального закона о персональных данных обусловило разработку различных подходов, связанных с выполнением требований к их защите и сокращением издержек на ее обеспечение. Одним из эффективных подходов к защите персональных данных является их обезличивание, поскольку оно позволяет снизить требования к уровню защищенности данных и, соответственно, сократить расходы на защиту. Поэтому процедуры обезличивания достаточно широко применяются на практике.

Обезличиванием персональных данных являются действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

К настоящему времени можно выделить, следующие методы обезличивания персональных данных:

– уменьшение перечня обрабатываемых сведений;

– замена части сведений идентификатором;

– замена численных значений минимальным, средним, или максимальным значением;

– понижение точности некоторых сведений;

– деление сведений на части и обработка в разных информационных системах.

Критерием качества метода обезличивания часто является возможность определить на основании имеющихся обезличенных данных конкретного человека, при учете контекста обработки, но часто возможно использование дополнительной информации из других источников, позволяющей провести деобезличивание.

Многие из перечисленных методов не гарантируют невозможность получения персональной информации (деобезличивания) путем использования контекста обработки и данных, размещенных в других системах, которые можно связать с обезличенными, поскольку эти методы, как правило, сохраняют связь между различными данными, относящимися к одному и тому же субъекту. Разорвать эту связь возможно, если осуществить перемешивание данных, относящихся к различным субъектам. Перемешивание данных имеет ряд достоинств, которые делают этот подход к обезличиванию достаточно перспективным:

– данные находятся в одном хранилище;

– использование дополнительных сведений, получаемых из других источников, не позволяет провести процедуру деобезличивания;

– простота реализации обезличивания и обратного формирования персональных данных;

– мобильность данных, позволяющая распространять их.

Для того что бы обезличивать персональные данные существуют требования и методы, которые определены в приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 5 сентября 2013 г. N 996 г.

Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных.

К свойствам обезличенных данных относятся: полнота; структурированность; релевантность; семантическая целостность; применимость; анонимность.

К характеристикам (свойствам) методов обезличивания персональных данных, определяющим возможность обеспечения заданных свойств обезличенных данных, относятся:

обратимость (преобразования, обратного обезличиванию, которое позволит привести обезличенные данные к исходному виду);

вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);

изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию субъекта персональных данных);

возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов);

совместимость (возможность интеграции персональных данных, обезличенных различными методами);

параметрический объем (объем дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);

возможность оценки качества данных (возможность проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

К требованиям к свойствам получаемых обезличенных данных относятся: сохранение полноты; сохранение структурированности обезличиваемых персональных данных; сохранение семантической целостности обезличиваемых персональных данных; анонимность отдельных данных не ниже заданного.

К требованиям к свойствам метода обезличивания относятся: обратимость (возможность проведения деобезличивания); возможность обеспечения заданного уровня анонимности; увели-

чение стойкости при увеличении объема обезличиваемых персональных данных.

Таким образом, обезличивание персональных данных является достаточно эффективным организационно-техническим способом обеспечения конфиденциальности персональных данных, позволяющим снизить затраты на эти цели.

Пономарева И.М.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Применение технических систем видеонаблюдения в деятельности ОВД

Системы видеонаблюдения как средство объективной фиксации различных процессов и явлений все шире используются в разных видах практической деятельности, в том числе и правоохранительной.

Предотвращение террористического акта на Таймс-сквер в Нью-Йорке 1 мая 2010 года, раскрытие взрывов, совершенных в Москве 29 марта 2010 года на станциях метро «Лубянка» и «Парк культуры», кражи крупной суммы денежных средств, совершенной в Минске 18 декабря 2009 года из пункта обмена валют ЗАО «Абсолютбанк» , во многом стали возможны благодаря тому, что все эти события были запечатлены камерами видеонаблюдения. Данные примеры свидетельствуют о том, что системы видеонаблюдения могут быть одним из эффективных средств, способствующих раскрытию, расследованию и предупреждению преступлений.

Под системой видеонаблюдения понимается комплекс объединенных линиями связи технических средств, предназначенных для видеонаблюдения за состоянием охраняемого объекта

(его части) и видеозаписи или подачи сигнала тревоги при изменении ситуации на нем.

Анализ нормативных правовых актов, правоприменительной практики позволяет условно выделить два направления использования стационарных систем видеонаблюдения в Российской Федерации: 1) охранная деятельность (телевизионные системы видеонаблюдения, системы охранного телевидения); 2) деятельность по обеспечению общественного порядка и безопасности на улицах и дорогах.

Несмотря на то, что задачи указанных направлений несколько отличаются, во всех случаях видеозапись, полученная с помощью систем видеонаблюдения, может быть использована как в оперативных целях (при установлении лица, совершившего либо готовящего преступление), так и в процессе доказывания по конкретному уголовному делу.

Раскрывая сущность первого направления, необходимо отметить, что в охранной деятельности системы видеонаблюдения используются для защиты имущества юридических и физических лиц от преступных посягательств, а также обеспечения безопасности персонала юридического лица.

Под обнаружением понимается необходимое отображение объекта на экране монитора, позволяющее однозначно установить, что в поле зрения телекамеры появился именно человек, а не птица, животное; автомобиль, а не телега, мотоцикл. Различение - это такое отображение объекта, которое дает возможность не просто обнаружить, например, человека, а определить его пол, возраст, одежду; если объект обнаружения - автомобиль, то распознать его марку, тип кузова и т.д. Идентификацией считается отождествление личности конкретного человека или установление конкретного транспортного средства.

К сожалению, на практике часто не выполняются все требования. Во многих случаях не ставятся задачи, которые должны решаться камерами видеонаблюдения. Для удешевления проекта используется аппаратура с низкой разрешающей способностью, которая справляется с функцией обнаружения и различения, но практически не позволяет идентифицировать объект.

Поэтому соблюдение законодательства в сфере охранной деятельности (особенно норм, устанавливающих стандарты и

технические требования к аппаратуре) способствует дальнейшему использованию результатов видеонаблюдения.

Другое значимое направление - использование систем видеонаблюдения в деятельности по обеспечению общественного порядка и безопасности на улицах городов и дорогах страны. Современное развитие городов невозможно без обеспечения общественной безопасности и поддержания правопорядка, предотвращения преступлений, в том числе актов вандализма, терактов, массовых беспорядков. Организация видеонаблюдения признается одной из важных составляющих осуществления таких мер. Системы видеонаблюдения активно используются для фиксации обстановки в местах скопления граждан (например, при проведении различных массовых мероприятий), контроля за дорожно-транспортной обстановкой и др.

Основные задачи применения систем видеонаблюдения - это обеспечение безопасности жителей городов и сохранности их имущества от преступных посягательств, охрана общественного порядка и контроль за обстановкой в городе, отслеживание транспортных потоков в реальном времени; фиксация обстоятельств совершения дорожно-транспортных происшествий и иных правонарушений; оперативное реагирование на противоправные действия; рациональное использование сил и средств нарядов милиции, несущих службу по охране общественного порядка.

Во многих европейских странах уже давно и достаточно широко с большим успехом применяют видеонаблюдение в целях борьбы с правонарушениями. Сигналы от видеокамер, установленных обычно совершенно открыто в местах наибольшего скопления людей или в криминогенных зонах, поступают на центральные пульты, записываются там и при необходимости используются позднее в качестве доказательного материала. По отзывам компетентных лиц, число преступлений в оборудованных таким образом местах заметно сократилось. Это несомненное достижение вкупе с разъяснительной работой среди населения способствовали тому, что граждане заинтересовались возможностями видеонаблюдения и применительно к своему собственному дому. Постепенно они признали все несомненные достоинства охранных систем разного рода и начали активно приобретать их,

несмотря даже на то что это иногда воспринималось как определенное вторжение в их личную жизнь.

Действующим российским законодательством производство видеозаписи в местах общего пользования напрямую не запрещено. Поскольку эта проблема является сравнительно новой для российского правосудия, споры о допустимости видеозаписей в каждом конкретном случае все еще носят несистемный характер. В то же время видеозаписи на законных основаниях могут использоваться в качестве доказательств.

Государство и частный сектор интенсивно используют новейшие средства видеонаблюдения в различных обстоятельствах и для различных целей. Несмотря на очевидные выгоды от видеонаблюдения, каждый, кто его осуществляет, должен отдавать себе ясный отчет в том, что оно должно быть обеспечено законными основаниями.

Без должных обоснований цели видеонаблюдения оно заведомо оказывается вне закона. Следует также помнить, что даже обоснованные цели могут не позволить использование полученных данных для других случаев, несмотря на их очевидность.

Наконец, следует помнить, что законность цели не существует в изоляции от конституционных прав граждан, в первую очередь от права на защиту частной жизни. Какой бы значимой ни была цель охраны собственности, достижение этой цели не допускает установки устройств видеонаблюдения в жилых помещениях (гостиных, спальнях, в ванных и туалетных комнатах и т.п.).

Системами видеонаблюдения могут быть задокументированы обстоятельства целого ряда преступлений - умышленной порчи имущества (ущерб в крупном размере), убийств, телесных повреждений, хищений и т.д. Ст. 81, ст. 84 Уголовного процессуального кодекса (УПК) РФ содержат положения, согласно которым видеозаписи являются документами, с помощью которых можно установить процесс совершения преступления, а также иные детали, относящиеся к уголовному делу. На практике в российских следственных и судебных органах видеозаписи в настоящее время широко используются в качестве доказательств в рамках уголовного процесса. Ст. 55 ч. 2 Гражданского процессуального кодекса (ГПК) РФ устанавливает, что в качестве доказательства в судебном разбирательстве могут использоваться ви-

деозаписи. Круг случаев, когда к гостинице, торговому центру или офисному комплексу могут быть поданы гражданские иски, достаточно широк (невежливое обращение с постояльцами, пищевое отравление посетителя в ресторане, неосторожное обращение с имуществом). В свою очередь, компания, которой принадлежат помещения с установленными в них видеокамерами, также может стать инициатором судебного разбирательства в отношении физических лиц (например, предъявление исков к своим работникам о возмещении ущерба). Российский Кодекс об административных правонарушениях (КоАП) в ст. 26.7 ч. 2 предусматривает возможность использования видеозаписей в качестве доказательств. Следовательно, в административном производстве по делам о мелком хулиганстве, порче имущества на незначительную сумму и т.д. будет допустимо использовать такие материалы. Арбитражного процессуального кодекса (АПК) РФ называет видеозаписи в качестве допустимых процессуальных доказательств. Ст. 24 Конституции Российской Федерации гласит: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются», а в комментариях к ней сказано: «Конституция, устанавливая право искать, получать, передавать, производить и распространять информацию в соответствии с международными нормами предусмотрела ограничения этого права, направленные на защиту личной жизни, уважение прав и репутации других лиц». Конституция устанавливает в качестве обязательного условия сбора, хранения, использования и распространения информации о частной жизни лица согласие этого лица. Конституция устанавливает общее правило, из которого существуют исключения, закрепленные в соответствующих законодательных актах. Так, не требуется согласия лица на сбор, хранение, использование и распространение сведений о нем при проведении следствия, дознания, оперативно-розыскных мероприятий. Порядок работы правоохранительных органов с информацией персонального характера регулируется процессуальным, а прежде всего уголовно-процессуальным, законодательством. Указанные органы не вправе выходить за рамки закона. В случае нарушения конституционного права личности на соблюдение порядка сбора, хранения, использования и

распространения информации персонального характера заинтересованное лицо вправе обратиться за защитой в судебные органы.

Рассмотрим теперь наиболее популярные юридические аспекты установки систем видеонаблюдения на предприятии, в офисе и т.п.

Согласно ч. 1 ст. 23 Конституции РФ каждый из нас имеет право на неприкосновенность частной жизни. Информацию о ней нельзя собирать, хранить, использовать и распространять без согласия человека (ч. 1 ст. 24 Конституции).[1] Однако многие руководители считают, что ничего личного на работе быть не может, и, устанавливая камеры в офисах, не спрашивают согласия сотрудников и вообще не ставят их в известность о видеонаблюдении. Согласно ст. 21 Трудового кодекса (ТК) РФ работник имеет право на полную информацию об условиях и охране труда на рабочем месте.

Такие доказательства в соответствии с ГПК должны обладать свойством допустимости (ст. 60 ГПК РФ). А в силу прямого указания закона доказательства, полученные с нарушением закона, не имеют юридической силы и не могут быть положены в основу решения суда (ч. 2 ст. 55 ГПК РФ)[2], т.е. такие доказательства свойством допустимости не обладают. По мнению суда, негласно полученная видеозапись не может являться основанием для наложения дисциплинарной ответственности на работника в виде увольнения (ст. 192,193 ТК РФ), а иных доказательств совершения работником дисциплинарного проступка работодатель не смог предоставить.

Таким образом, организация видеонаблюдения в офисе или производственном помещении требует соблюдения многих условий. В противном случае работодатель может оказаться в различных неприятных ситуациях – от потери лояльности сотрудников, узнавших о системе слежения по слухам, до проигрыша дела в суде.

---

[1]Конституция рф 1993 г

[2]Гражданский процессуальный кодекс российской федерации (гпк рф) от 14.11.2002 n 138-фз

Раздобудина А.А.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Геоинформационная система в деятельности дежурных частей ОВД

В последние годы благодаря стремительному развитию и совершенствованию программно-технических возможностей работа с информацией достигла такого уровня, который еще десять-пятнадцать лет назад трудно было даже представить. Многообразие задач решаемых с использованием информационных систем, инициировало появление разнотипных систем. Соответственно, они отличаются между собой принципами построения, правилами хранения, сочетание и представления информации в виде, наиболее удобном для потребителя. Необходимость получения реального представления о пространственном размещении отдельных объектов, от которых зависит оперативная обстановка, с использованием карт или планов инициировало появление геоинформационных систем. Создание корпоративной геоинформационной системы (электронной карты), которая на новом уровне позволит решать следующие задачи: создание централизованной системы поиска мобильного объекта и сопровождение его траектории движения по электронной картой; графическое представление расстановки сил и средств на территории позволит сокращение времени прибытия на место происшествия сотрудников полиции[1].

Удобство наглядного восприятия пространственного размещения объектов на определенной территории с использованием карты и ранее, в «докомпьютерную» эпоху, инициировала такое

[1]В.А. Гвоздева, И. Ю. Лаврентьева. - М.: ИД «ФОРУМ»: ИНФРА-М, 2007. – 320 с. с. 79-84

сочетание. Историческими предшественниками геоинформационных систем в органах внутренних дел можно считать карты городов, районов на которых в дежурных частях и штабных подразделениях с помощью условных фигур в ручном режиме отображались места совершения преступлений, нахождения нарядов милиции и др.. Но полноценно реализация этой цели стало возможным благодаря привлечению для обработки информации компьютерной техники и телекоммуникационных сетей. Компьютерные технологии и сети современной связи предоставили условия для постоянного отслеживания, в реальном времени мест нахождения определенных объектов на электронных изображениях карт с различных устройств ввода, а сочетание карт с базами данных информации об определенных объектах составило реальные условия оценки оперативной обстановки в городе, районе, в отдельном участке и др.. Вехов В.Б. называет такие системы автоматизированными, информационно-мониторинговыми и говорит, что они позволяют - «определять местоположение объектов охраняемых или тех контролируемых (транспортных средств, лиц, животных, грузов) путем их статического или динамического отображения на электронной карте местности (на дисплее мобильного или стационарного терминала) »[1].

Попробуем определиться, что же представляют собой геоинформационные системы вообще, в чем состоит основа их построения и возможности совершенствования работы с информацией. В Законе «О Национальной программе информатизации» говорится: «Геоинформационные системы - современные компьютерные технологии, позволяющие соединить модельное изображение территории (электронное отображение карт, схем, космо-, аэроизображение земной поверхности) с информацией табличного типа (разнообразные статистические данные, списки, экономические показатели и т.д.)»[2]. Вряд такое определение можно считать совершенным. Не будем подробно останавливаться на анализе его содержания, но заметим, что когда речь идет об

[1]Вехов В.Б. Основы криминалистического учения о исследовании и использовании компьютерной информации и средств ее обработки: [монография] /В.Б. Вехов. - Волгоград: ВА МВД России - 404с. с.340

[2]Денисова А.А. Информационные системы и технологии в юридической деятельности: [учеб. пособие] /А. Денисова. -К. : КНЭУ, 2003. - 315 с.

информационной системе целесообразно определять ее именно как систему с описанием составляющих и уже потом можно добавить средства и технологии обработки информации, составляющей ее базы данных. Гвоздева В. А. и Лаврентьева И. Ю. полагают, что «геоинформационные системы - системы, в которых все данные об объектах привязаны к общей электронной топографической основы. Эти системы предназначены для использования в тех предметных областях, в которых структура объектов и процессов, имеющих пространственно-географическую привязку»[1]. Без преувеличения можно сказать, что приведенное определение более понятным.

Геоинформационные системы представляют собой сложные информационные системы создаваемые благодаря интеграции массивов обычной (чаще фактографической) информации относительно объектов учета, с массивами географической (топографических карт, планов и др.). Главное отличие ГИС - связь между геометрией картографической информации и атрибутивными данными в табличной форме. Эта связь дает возможность переходить от одного представления данных к другому или соединять их. Такое сочетание баз данных создает условия для получения представления о пространственного размещения по определенным координатам (географическими или специфическими) объектов учета, что в свою очередь активно воздействует на анализ и синтез учетной информации, стимулирует принятия взвешенных решений. Не вызывает сомнения, что без применения ГИС обобщения и полноценный анализ атрибутивной информации по объектам информационных систем по их пространственным расположением достаточно сложным, это в свою очередь влияет на обоснование и принятия оптимальных решений. Главным преимуществом, предоставляющих ГИС является возможность визуализации информации, содержащейся в традиционных базах данных с привязкой к электронным изображений карт, с целью их географического (пространственного) анализа. Именно с помощью ГИС можно получить наглядное представление об этих данных. «Даже простейшие электронные карты повышают достовер-

[1]Гвоздева В.А., Лаврентьева И. Ю. Основы построения автоматизированных систем / с.19

ность информации о подведомственный территорию за счет привязки к картографической базы данных и наглядного ее отражение. Это дает возможность облегчить анализ информации о правонарушениях, оперативно принять решение по принятию мер с учетом особенностей территории, оптимизировать силы и средства, проконтролировать движение мобильных объектов, направить патрули и т.д.»[1].

Информационную основу относительно объектов ГИС составляет информация обычных информационных систем, функционирующих в подразделениях МВД на определенном уровне, соответственно и основу картографической базы данных составляют электронные карты и планы определенной территории. Эти системы можно классифицировать на местные, региональные и центральные. Причем они могут быть как совмещенными в сеть на каком-то уровне, так и представленными в локальном виде, даже в одном локальном программно-аппаратном комплексе.

Использование ГИС создает условия для решения вопросов в двух принципиально противоположных направлениях. Первыми являются вопросы типа - какие объекты находятся в определенном месте (в определенной на карте территории)? В зависимости от запроса можно получить информацию о людях, ранее судимых обитающих на указанной территории, пострадавших и без вести пропавших месту нахождения которых была и территория, о преступлениях которые были совершены в ее пределах, о наличии и качестве оперативного перекрытия, а также саму разнообразную информацию из интегрированных в ГИС информационных систем. Вторым - где находятся определенные объекты? Такие вопросы возникают когда необходимо определиться с пространственным размещением определенных объектов, взятых на учет. Ответ отображается визуально в виде символа, объект в определенном городе на карте. Говоря о возможности использования геоинформационных систем в борьбе с преступностью Курин А. подчеркивает, что «существенное значение современные технологии приобретают в деятельности правоохранительных ор-

[1]Информационные технологии в оперативно-служебной деятельности органов внутренних дел Луганской области /Гуславский В.С., Задорожный Ю.А., Андреев М.В. и др. - Луганск: РИО Лавдей - 84 с.

ганов, которые особенно заинтересованы в достоверной информации. Быстро получена, такая информация позволяет в короткие сроки установить связи между отдельными участниками преступления, получить информацию о местоположении членов преступной группы и принимать управленческие решения в рамках оперативно-розыскных мероприятий и следственных действий»[1]. Сейчас в космическом пространстве развернуты две крупнейшие навигационные системы глобального позиционирования (Global Positioning System - GPS), оставшиеся в наследство от эпохи холодной войны : отечественная ГЛОНАСС и американская НАВСТАР/ (NAVSTAR).

Системы обеспечивают:

- глобальность, т.е. возможность осуществлять навигационные операции в любой точке Земли и околоземного космического пространства в любое время суток независимо от погоды;

- точность определения местонахождения с погрешностью не более 100 м. и скорости не более 15 см/сек, при переходе в так называемый дифференциальный режим работы определенные погрешности координатной привязки не превышают нескольких метров;

- независимость навигационных операций применительно к различным потребителям;

- оперативность проведения навигационных операций с погрешностью привязки к шкале единого времени не более 1мкс.

Охарактеризуем более детально значение и роль синтеза космических навигационных систем и геоинформационных систем для решения задач оперативного управления в органах внутренних дел.

Географическая пространственная информация - исключительно ценный продукт и товар в наше перегруженное информацией время. Переиначивая известный афоризм, можно утверждать: кто владеет ею, тот владеет ситуацией и имеет шансы избежать ошибок при принятии политических, экономических, экологических, криминологических и правовых решений, улажива-

[1]Курин А.А. Геоинформационные технологи в функционировании системы криминалистической регистрации /А. А. Курин //Информационное обеспечение правоохранительной деятельности: проблемы тенденции перспективы: сб. научн. ст. - Калининград: Калининградский ЮИ МВД России, 2007. - С. 136-142.

нии региональных конфликтов, реализации различных проектов и программ.

Эволюцию ГИС в управлении органами внутренних дел и внутренними войсками можно условно разбить на три этапа. Первый этап - это создание многочисленных систем, представлявших собой, по существу, автоматизированные топографические карты. Второй этап - отображаемая на экране карта (пока все еще плоская) стала утрачивать первостепенное значение. Она стала выполнять функции графического интерфейса пользователя, обеспечивающего доступ к информационным ресурсам. В первую очередь, к базам данных. Именно на этом этапе ГИС становятся полноценными информационными системами. Третий этап связан с тем, что информационные функции в ГИС дополняются аналитическими. ГИС уже позволяет не только наглядно отображать имеющуюся информацию, но и решать сложные расчетные задачи оперативного управления в ОВД и ВВ, требующие разнородных исходных данных.

Новые задачи требовали пространственных моделей и средств, позволяющих хранить и манипулировать векторными и растровыми данными и даже видеофрагментами.

К сожалению, в России рынок высокопроизводительных ГИС пока невелик. Тем более невелико их количество, используемое в оперативном управлении ОВД. Но эффективность использования спутниковых навигационных систем в значительной степени зависит от возможности их совместного использования с электронными картами. Поэтому большой интерес представляют ГИС, объединенные с навигационными и спутниковыми системами.

Подводя итоги сказанному, отметим геоинформационные системы (ГИС) представляют сложные информационные системы сочетающие в себе базы данных обычных автоматизированных информационных систем с базами данных картографической информации; сегодня эти системы представляют резерв по совершенствованию работы по раскрытию преступлений и организации управленческой деятельности.

Эффективность использования возможностей ГИС в практической деятельности по расследованию преступлений напрямую зависит от их приближения к непосредственным потребите-

лям информации. Процессы формирования таких систем, а также их использование в практической деятельности непосредственно зависят от степени их теоретического осмысления на научном уровне.

Сокуров Б.Х.,
слушатель 5 курса
Краснодарского университета МВД России
Научный руководитель:
Белый А.Г.,
кандидат юридических наук
доцент кафедры ОРД в ОВД
Краснодарского университета МВД России

Проблемы предупреждения террористических актов в отношении представителей силовых структур

Вопросы противодействия террористической деятельности приобрели в современном обществе особую актуальность. Деятельность экстремистских организаций и группировок в настоящее время продолжает оставаться серьезным фактором дестабилизации социально-политической ситуации в России и представляет собой серьезную угрозу конституционной безопасности и территориальной целостности страны.

В современной практике террористической деятельности в последнее время получил широкое распространение терроризм в отношении представителей силовых структур. Он характеризуется особой жестокостью, большим числом человеческих жертв. Нападения на блок-посты и отделения полиции в Дагестане и Ингушетии стали повседневной реальностью.

Наибольшее распространение получили следующие способы совершения актов терроризма в отношении представителей силовых структур:

угроза по телефону (телефонный терроризм);

демонстративная закладка муляжей взрывчатых веществ и взрывных устройств;

скрытая закладка бомбы на объекте и ее взрыв;

взрыв припаркованного автомобиля с террористом смертником;

подбрасывание закамуфлированных под бытовые предметы мин-ловушек;

засылка конкретному адресу бомбы в почтовом отправлении[1].

Противодействие терроризму в отношении представителей силовых структур в Российской Федерации должно, на наш взгляд, осуществляться по следующим направлениям:

а) предупреждение (профилактика) терроризма;

б) борьба с терроризмом;

в) минимизация и (или) ликвидация последствий проявлений терроризма.

Предупреждение (профилактика) терроризма должна осуществляться по трем основным направлениям:

а) создание системы противодействия идеологии терроризма;

б) осуществление мер правового, организационного, оперативного, административного, режимного, военного и технического характера, направленных на обеспечение антитеррористической защищенности представителей силовых структур - потенциальных объектов террористических посягательств;

в) усиление контроля за соблюдением административно-правовых режимов[2].

Особая роль в предупреждении (профилактике) терроризма в отношении представителей силовых структур принадлежит эффективной реализации административно-правовых мер, предусмотренных законодательством Российской Федерации.

Предупреждение (профилактика) терроризма в отношении представителей силовых структур предполагает решение следующих задач:

а) разработка мер и осуществление мероприятий по устранению причин и условий, способствующих возникновению и распространению терроризма;

б) противодействие распространению идеологии терроризма путем обеспечения защиты единого информационного простран-

---

[1]Кожушко Е. Современный терроризм. Анализ основных направлений. – Мн.: Харвест, 2010. – 447с.

[2]Ольшанский Д.В. Психология терроризма. – СПб.: Питер, 2010, - 286 с.

ства Российской Федерации; совершенствование системы информационного противодействия терроризму;

в) улучшение социально-экономической, общественно-политической и правовой ситуации в стране;

г) прогнозирование, выявление и устранение террористических угроз в отношении представителей силовых структур, информирование о них органов государственной власти, органов местного самоуправления и общественности;

д) использование законодательно разрешенных методов воздействия на поведение отдельных лиц (групп лиц), склонных к действиям террористического характера в отношении представителей силовых структур;

е) разработка и введение в действие типовых требований по обеспечению защищенности от террористических угроз представителей силовых структур.

ж) совершенствование нормативно-правовой базы, регулирующей вопросы возмещения вреда, причиненного жизни, здоровью и имуществу представителей силовых структур, участвующих в борьбе с терроризмом, а также лиц, пострадавших в результате террористического акта;

з) усиление взаимодействия федеральных органов исполнительной власти и укрепление международного сотрудничества в области противодействия терроризму против представителей силовых структур;

и) обеспечение скоординированной работы органов государственной власти с общественными и религиозными организациями (объединениями), другими институтами гражданского общества и гражданами.

Организация борьбы с терроризмом против представителей силовых структур должна осуществляться на основе комплексного подхода к анализу причин его возникновения и распространения, к выявлению субъектов террористической деятельности, четкого разграничения функций и зоны ответственности субъектов противодействия терроризму, своевременного определения приоритетов в решении поставленных задач, совершенствования организации и взаимодействия оперативных, оперативно-боевых, войсковых и следственных подразделений путем внедрения штабного принципа организации управления контртеррористиче-

скими операциями и обеспечения указанных субъектов информационными ресурсами, включающими современные аппаратно-программные комплексы[1].

Одно из основных условий повышения результативности борьбы с терроризмом против представителей силовых структур - получение упреждающей информации о планах террористических организаций по совершению террористических актов, деятельности по распространению идеологии терроризма, источниках и каналах финансирования, снабжения оружием, боеприпасами, иными средствами для осуществления террористической деятельности.

Условием эффективной организации борьбы с терроризмом против представителей силовых структур является заблаговременная подготовка сил и средств субъектов противодействия терроризму к пресечению террористического акта в ходе командно-штабных, тактико-специальных, оперативно-тактических учений, организуемых Федеральным оперативным штабом и оперативными штабами в субъектах Российской Федерации[2].

Деятельность по минимизации и (или) ликвидации последствий проявлений терроризма против представителей силовых структур планируется заблаговременно исходя из прогнозов возможных последствий террористических актов. Эта деятельность должна быть ориентирована на решение следующих основных задач:

а) недопущение (минимизация) человеческих потерь исходя из приоритета жизни и здоровья человека над материальными и финансовыми ресурсами;

б) своевременное проведение аварийно-спасательных работ при совершении террористического акта, оказание медицинской и иной помощи лицам, участвующим в его пресечении, а также лицам, пострадавшим в результате террористического акта, их последующая социальная и психологическая реабилитация;

в) минимизация последствий террористического акта и его неблагоприятного морально-психологического воздействия на представителей силовых структур;

---

[1]Лазарев И.М. Терроризм как тип политического поведения // Социс. – 2009.- № 6.

[2]Колобов О.А. Терроризм и контртерроризм в современном мире: Аналитические материалы, документы, глоссарий: Научно-справочное издание. Экслит, 2008.

г) восстановление поврежденных или разрушенных в результате террористического акта объектов;

д) возмещение в соответствии с законодательством Российской Федерации причиненного вреда физическим и юридическим лицам - представителям силовых структур, пострадавшим в результате террористического акта[1].

В соответствии с основными направлениями противодействия терроризму против представителей силовых структур должна осуществляться посредством системы мер, в ходе реализации которых используются различные взаимосвязанные и согласованные между собой формы, методы, приемы и средства воздействия на субъекты террористической деятельности.

При осуществлении деятельности по предупреждению (профилактике) терроризма против представителей силовых структур применяются меры, направленные на снижение уровня угроз террористических актов, урегулирование экономических, политических, социальных, национальных и конфессиональных противоречий, которые могут привести к возникновению вооруженных конфликтов и, как следствие, способствовать террористическим проявлениям; предупреждение террористических намерений граждан; затруднение действий субъектов террористической деятельности. При этом используются различные формы общей и адресной профилактики, осуществляемой с учетом демографических, этноконфессиональных, индивидуально-психологических и иных особенностей объекта, к которому применяются меры профилактического воздействия[2].

К основным мерам по предупреждению (профилактике) терроризма относятся:

а) политические (нормализация общественно-политической ситуации, разрешение социальных конфликтов, снижение уровня социально-политической напряженности, осуществление международного сотрудничества в области противодействия терроризму);

б) социально-экономические (оздоровление экономики регионов Российской Федерации и выравнивание уровня их разви-

---

[1]Кожушко Е. Современный терроризм. Анализ основных направлений. – Мн.: Харвест, 2010. – 447с.

[2]Колобов О.А. Терроризм и контртерроризм в современном мире: Аналитические материалы, документы, глоссарий: Научно-справочное издание. Экслит, 2008.

тия, сокращение масштабов маргинализации общества, его социального и имущественного расслоения и дифференциации, обеспечение социальной защиты населения);

в) правовые (реализация принципа неотвратимости наказания за преступления террористического характера, незаконный оборот оружия, боеприпасов, взрывчатых веществ, наркотических средств, психотропных веществ и их прекурсоров, радиоактивных материалов, опасных биологических веществ и химических реагентов, финансирование терроризма, а также регулирование миграционных процессов и порядка использования информационно-коммуника-ционных систем);

г) информационные (разъяснение сущности терроризма и его общественной опасности, формирование стойкого неприятия обществом идеологии насилия, а также привлечение граждан к участию в противодействии терроризму);

д) культурно-образовательные (пропаганда социально значимых ценностей и создание условий для мирного межнационального и межконфессионального диалога);

Основной формой пресечения террористического акта против представителей силовых структур является контртеррористическая операция, которая предусматривает реализацию комплекса специальных, оперативно-боевых, войсковых и иных мероприятий с применением боевой техники, оружия и специальных средств по пресечению террористического акта, обезвреживанию террористов, обеспечению безопасности представителей силовых структур, организаций и учреждений, а также по минимизации и (или) ликвидации последствий проявлений терроризма.

Стельмаков С.С.,
слушатель 5 курса
Краснодарского университета МВД России
Научный руководитель:
Калюжный К.Ю.,
старший преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России

Проблемы пресечения финансирования террористических организаций

В течение долгого времени терроризм был одним из ведущих факторов, определяющих взрывоопасную ситуацию, которая царит на Ближнем Востоке на протяжении почти всего XX в. и имеет место и в наше время. Выявление экономических основ, которые позволяют террористическим организациям в этом регионе активно действовать и расширять свою сеть, может помочь более точно оценить их потенциал и способность слаженно и в максимальной степени осуществлять свои задачи, а, значит, усилить борьбу с этими сообществами. К числу основных источников получения финансовых средств террористических организаций на Ближнем Востоке следует отнести:

незаконные и неконтролируемые операции в финансовой сфере (в частности, в банковской);

криминал; совместную деятельность преступных сообществ;

деятельность легальных организаций (коммерческих предприятий);

деятельность «благотворительных» и «гуманитарных» организаций;

спонсорскую помощь государственных структур отдельных стран этого региона;

личные состояния ряда представителей террористических организаций и т.д.

Одними из наиболее ярких и драматичных террористических актов, совершенных в XX в., стали нападения на здания Всемирного торгового центра и Пентагона, произошедшие 11 сентября 2001 г. в США. Будучи беспрецедентными, по своей

сути, эти события вызвали много вопросов, к числу которых относятся следующие: какие средства могли быть затрачены на проведение подобной акции? Каковы источники этих средств? Каков масштаб деятельности организации или организаций, которые смогли осуществить эти теракты?

По данным ФБР США, приблизительная сумма, которая была затрачена на осуществление этого теракта, варьируется между 300–500 тыс. долл. С самого начала расследование событий 11 сентября установило связь между террористами, находившимися в четырех самолетах, и их соучастников с финансовыми источниками, расположенными в странах Персидского залива, Германии и некоторых других государствах Западной Европы. В качестве ключевых членов организации «Аль-Каида» и одновременно распорядителей денежных средств были названы, в частности, Рамзи бен аш-Шибх в Германии и Мустафа Ахмед аль-Хаснауи в Объединенных Арабских Эмиратах. Анализ финансовой деятельности этих людей подтвердил, что террористические акты 11 сентября были осуществлены организацией «Аль-Каида». Установлена связь между преступниками, непосредственно совершившими нападения, другими членами организации, оказывавшими им поддержку из Германии, в частности, с Захарием Мусауи. Телефонные и телеграфные контакты между Мусауи и Бен аш-Шибхом сыграли решающую роль в обвинении Мусауи в участии в терактах 11 сентября. Финансовые расследования также установили связь между Мусауи и членами «Аль-Каиды», связанными с малазийской организацией «Джамаа аль-Ислами».

Банковские системы включены в финансирование террористических организаций во многих странах мира. Отделения «Арабского Банка» используются некоторыми террористическими организациями, подобными «Хамас» (особенно его дамасским филиалом), для перевода средств на счета своих сторонников для оплаты террористических операций, в частности, проводящихся и на Западном берегу реки Иордан. Некоторые из активистов «Хамас» такие, как Табит Мардауи и Али Саффури, были задержаны спецслужбами Израиля. В ходе расследования их деятельности выяснилось, что этими лицами было открыто несколько банковских счетов, на которые переводились средства, шедшие через «Арабский банк». Во время рейдов израильских войск на оккупи-

рованных территориях на Западном берегу реки Иордан представителями спецслужб Израиля были обнаружены документы, которые являлись неопровержимым подтверждением факта передачи саудовскими организациями денег структурам, связанным с «Хамас» и семьями террористов-смертников, через отделения «Арабского Банка», расположенные на Западном берегу реки Иордан. В качестве другого примера можно привести использование «Арабского Банка» полковником Муниром аль-Макда, также известным как Абу Хасан, для передачи средств отделению движения «Фатх» – «Бригаде мучеников аль-Аксы». Начиная с середины 2001 г., аль-Макда перевел приблизительно 40–50 тыс. долл. на счет Насера Увайса, одного из лидеров «Фатх». По некоторым данным, эти средства пошли на закупку оружия, оборудования, транспорт и на другие расходы для осуществления терактов как на территории Израиля, так и за его пределами. «Арабский Банк» аккумулировал и переводил средства не только на территории стран Ближнего Востока. Используя возможности этого банка, ряд лиц, подозреваемых в причастности к деятельности «Аль-Каиды», переводили средства из Испании в Пакистан и Йемен.

14 декабря 2003 г. в газете «Вашингтон Пост» был опубликован детальный отчет о проведении федеральными органами США операции по блокированию финансовых средств физических и юридических лиц, подозреваемых или обвиненных в причастности к деятельности террористических организаций. В ходе этой операции было арестовано и обвинено в пособничестве террористическим организациям 272 человека, 138 млн. долл. были заморожено на счетах этих и других лиц, находящихся в федеральном розыске или розыске международных организаций. Из 138 млн. долл. 75 млн. были размещены на счетах «Аль-Каиды». Часть средств, арестованных федеральными властями, принадлежала также «Организации помощи улемов». Штаб-квартира и основные базы этой организации расположены в Пакистане. В 1999 г. именно эта организация занималась сбором средств для афганских талибов. После начала совместных действий антитеррористической коалиции администрация Буша отнесла эту организацию к числу наиболее важных структур, занимающихся финансированием различных террористических группировок, включая

и «Аль-Каиду». Наряду со счетами этой организации были арестованы счета физических лиц, к числу которых относились:

Аль-Фауаз Халид в 1994 г. был направлен Усамой бен Ладеном в Лондон, где открыл офис с целью координации действий отделений «Аль-Каиды» на территории Великобритании и за ее пределами. Подозревается в участии в организации взрывов американских посольств в Кении и Танзании.

Аль-Масри Абу Хамза заявляет о себе, как об офицере «Исламской Армии Адена», террористической организации, которая была причастна к серии взрывов в Йемене в середине 90-х годов XX в. 24 сентября 2001 г. президент США назвал эту организацию одним из источников финансирования терроризма на Ближнем Востоке и за его пределами.

Уади Мохаммед бен Белькасем член организаций «Салафитская группа Проповеди и Джихада» и «Аль-Каида». Был арестован в Италии и приговорен к пятилетнему тюремному заключению за торговлю и транспортировку оружия и взрывчатых веществ. Он также участвовал в передаче фальшивых документов другим членам «Аль-Каиды», действовавшим на территории Италии.

Одним из главных способов получения денежных средств представителями террористических организаций и групп является криминал. Контрабанда, похищения людей, вымогательство, продажа наркотиков, подделка документов и т.п. – все это неполный перечень приемов получения финансовых средств террористическими группами и сообществами. Для осуществления своей деятельности «Аль-Каида» и «Хизбалла» добывают большую часть средств продажей наркотиков. По некоторым данным, 35% средств, которые находятся в распоряжении «Аль-Каиды», получены именно от этого вида преступной деятельности. Многие данные указывают на то, что основные базы по производству и переработке наркотиков, контролируемые «Аль-Каидой», находятся в Афганистане. «Хизбалла» же контролирует продажу наркотиков в Ливане, используя полученные от продажи финансовые средства на поддержку своих сторонников на оккупированных Израилем территориях. Для получения дополнительных доходов «Хизбалла» и другие террористические организации организуют и контролируют пути доставки наркотиков в США и

страны Западной Европы. Международное Агентство по борьбе с наркотиками (АБН) провело расследование, имевшее целью установить пути распространения различных наркотиков, а также степень участия представителей таких стран, как Иран, Иордания, Йемен, Ливан, Сирия и таких террористических организаций, как «Хизбалла» и «Хамас» в этом процессе. По окончании расследования глава АБН Аса Хатчинсон заявила, что большая часть доходов от продажи наркотиков идет на нужды террористических организаций.

Организации «Хизбалла» и «Хамас» также активно действуют на черных рынках золота и драгоценных камней. По словам официальных лиц, в последнее время в Конго наблюдается «приток» главным образом исламских экстремистов, которые самым активным образом участвуют в контрабанде алмазов. При этом, террористические группы получают вооружение по схеме «оружие в обмен на алмазы». Бельгийские власти выдали постановление об аресте Виктора Бута, известного торговца оружием, который подозревался в поставках вооружения движению Талибан и «Аль-Каиде», а также различным воюющим группировкам по всей Африке.

По некоторым данным, источником получения средств для террористических организаций также является производство и распространение нелицензионных копий компьютерных программ, музыкальной и видеопродукции, распространяемой на CD и DVD дисках. Пиратское использование охраняемой законом интеллектуальной собственности ежегодно приносит миллионы долларов не только непосредственно производителям и распространителям контрабандной продукции, но также и представителям и террористических группировок, которые получают финансовые средства в виде «лицензионных платежей» – своеобразной дани, которой они облагают всех производителей пиратских копий продукции мультимедиа. По некоторым данным, члены таких организаций, как «Фатх», «Хамас», а также Палестинской Национальной администрации получают финансовые средства подобным образом.

Для прикрытия различных видов незаконной деятельности террористических структур привлекаются некоторые гуманитарные и благотворительные организации. Проведение расследова-

ния в подобных ситуациях представляется крайне затруднительным, поскольку затрагивает организации, которые могли быть случайно втянуты в деятельность преступных организаций и действовали непреднамеренно наряду с теми организациями, которые были образованы исключительно для поддержки террористических организаций и работали под маркой благотворительных.

Задолго до трагических событий 11 сентября 2001 г., которые стимулировали объединение усилий многих стран мира в борьбе против терроризма, различные международные и национальные правоохранительные организации представляли доклады, в которых высказывались предположения или непосредственно указывалось на участие некоторых благотворительных и гуманитарных фондов в деятельности, несовместимой с целями, заявленными в их уставах. В ходе расследований взрывов в Центре международной торговли (США) в 1993 г. была установлена причастность к этим событиям одной гуманитарной организации, занимавшейся поставками сувенирной продукции из Мекки (Саудовская Аравия) в Пакистан. В 1997 г. канадское правительство прекратило оказание поддержки «Хьюмен Консён Интернэшнл». Эта организация работала в основном на территории Канады и США. Причиной принятия такого решения послужило расследование ее деятельности и обвинение в содействии террористическим организациям.

Некоторые благотворительные и гуманитарные фонды используются международными террористами не только с целью получения и отмывания денежных средств, но также для облегчения их деятельности благодаря использованию статуса этих организаций, который предоставляет определенные льготы. С этим столкнулись американские военные в ходе своих операций в Афганистане и Ираке, когда подозреваемые ими в поддержке террористов лица предъявляли документы гуманитарных организаций. Следует отметить, что американские военные под предлогом проведения контртеррористических операций не раз совершали противоправные действия в отношении активистов гуманитарных и благотворительных организаций, тем самым препятствуя оказанию помощи крайне нуждающимся в ней народам Афганистана и Ирака.

В конце XX – начале XXI вв. одна из задач государства – охрана своих граждан от действий преступных организаций (в

частности, осуществляющих террористическую деятельность), используя для этого весь арсенал средств, находящийся в его распоряжении и обеспечивающий профилактику, сдерживание и защиту, – стала одной из наиболее актуальных. Возможность полного уничтожения терроризма представляется, к сожалению, маловероятной. Однако то, что терроризм не может быть полностью искоренен, не означает, что следует отказаться от осуществления мер, препятствующих его распространению. В этом отношении выявление источников финансирования деятельности террористических организаций способствует не только расследованию причин тех или иных террористических актов, но и предотвращению других подобных противоправных деяний, ведущих к большим человеческим и материальным потерям. В частности, расследование терактов 11 сентября 2001 г. в США, финансирования их организации и осуществления способствовало не только раскрытию некоторых отдельных участников преступного заговора, но и связей террористической организации «Аль-Каида» с другими преступными сообществами, действующими в различных странах мира, в том числе и на Ближнем Востоке.

Сорокина И.И.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Понятие служебной тайны и правовые основы ее защиты

Рассматриваемый вид информации ограниченного доступа существует достаточно продолжительное время. Анализ современной ситуации в России свидетельствует о том, что недостаточное правовое регулирование процессов обмена информации

приводит к тому, что сведения, имеющие ограниченный доступ, становятся общедоступными. Это ставит под угрозу безопасность государства, а также граждан и организации и при этом наносит им серьезный ущерб. Что касается служебной тайны, то существуют проблемы, связанные с отсутствием четкого определения, а также перечня информации, которую следует относить к этому виду тайны.

Необходимость изучения данного вопроса определяется тем, что правовое регулирование, четкий понятийный аппарат, создание нормативных актов позволят избежать таких проблем как распространение и предоставление несанкционированным субъектам информации, составляющей служебную тайну.

Рассматривая нормативно-правовые акты, такие как Федеральные Законы, Гражданский Кодекс, очевидно наличие противоречий в законодательстве. Проблеме защиты служебной тайны посвящено много публикаций, в которых предлагаются методы решения этих проблем.

Прежде чем приступить к рассмотрению проблемы, необходимо провести обзор толкования ключевых терминов в справочной литературе, нормативно правовых актах – это будет способствовать более глубокому изучению данной темы.

Согласно словарю русского языка С.И. Ожегова тайна – это нечто скрываемое от других, известное не всем, секрет.

Что же касается понятия служебная тайна, то в законодательстве оно однозначно не определено. Анализ нормативных актов позволил нам выявить содержание, особенности и основные признаки отнесения информации к служебной тайне.

Впервые законодательно урегулировал тайну и ввел ответственность за ее разглашение на Руси Петр I. До начала XVIII века существовала только тайна исповеди. Эти отношения регулировались «Духовным регламентом о праве чина церковного и монашеского».

Первые нормы по защите информации - запрет ее разглашения, под страхом смерти были регламентированы Петром I в Артикуле воинском (1715 г.) и Уставе морском (1720 г.).

Законодательство регулирования тайны в Российской империи и ответственность за ее распространение сформировалось лишь к середине XIX - началу XX века. Появилась правовая за-

щита тайны частной жизни, профессиональной тайны врачей, адвокатов, нотариусов, фабричной и торговой (коммерческой) тайны. В 1845 году Россия ввела наказание за разглашение коммерческой тайны.

Гражданский кодекс Российской Федерации, принятый 21 октября 1994 года, стал серьезным шагом на пути развитии информационного права. Отечественный законодатель признал информацию самостоятельным объектом права (ст. 128), дал определение коммерческой и служебной тайны (ст. 139).

До 1января 2008 года в составе статьи 139 Гражданского кодекса Российской Федерации существовало понятие «служебная тайна» и «коммерческая тайна», но законодатель не проводил между ними различия. «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами».

То же самое можно сказать и о служебной тайне. Находясь в прямой связи с государственной тайной, она не имеет однозначного определения. В результате чего в действующем законодательстве отсутствуют нормативные акты, в которых сформулирован институт служебной тайны. Информация, содержащая служебную тайну, может не носить коммерческий характер, но иметь немалую стоимость.

Служебная тайна близка по смыслу с профессиональной тайной, но главной отличительной особенностью является, то, что такие сведения непосредственно относятся к деятельности органов государственной власти, которые устанавливают ее правовой режим. Другими словами, информация, относящаяся к служебной тайне – это государственные секреты, носителями которых являются все служащие, в органах государственной власти. Но в зависимости от того, кто является владельцем информации, она может менять свой правовой статус.

Для того чтобы разобраться в существе служебной тайны, обратимся к утвержденному постановлением Правительства РФ

от 03.11.94 №1233 Положению о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. В соответствии с указанным постановлением к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью. Носители информации, составляющей служебную тайну, имеют пометку «Для служебного пользования». Однако складывается парадоксальная ситуация. После отмены с 01.01.2008 Федеральным законом от 18.12.2006 N 231-ФЗ статьи 139 «Служебная и коммерческая тайна» части первой Гражданского кодекса от 30.11.1994 № 51-ФЗ ни одним Федеральным законом доступ к служебной тайне не ограничивается. Таким образом, складывается парадоксальная ситуация. Служебную тайну нельзя признать информацией ограниченного доступа, несмотря на наличие требований по ее защите в подзаконных нормативных актах.

Одним ведомственных документов, отражающих понятие служебная тайна, является Федеральный закон от 30.11.2011 N 342-ФЗ «О службе в органах внутренних дел РФ и внесении изменений в отдельные законодательные акты РФ». В статье 12 данного закона (Основные обязанности сотрудника органов внутренних дел) сказано, что сотрудник органов внутренних дел обязан не разглашать сведения, составляющие государственную и иную охраняемую законом тайну, а также сведения, ставшие ему известными в связи с выполнением служебных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство.

В соответствии со ст. 23 в контракте, подписываемом сотрудником органов внутренних дел при поступлении на службу, предусматривается условие неразглашения сотрудником органов внутренних дел сведений, составляющих государственную и иную охраняемую законом тайну, конфиденциальной информации (служебной тайны)

Исходя из текста присяги (ст. 28), служебная тайна не подлежит разглашению сотрудниками органов внутренних дел Российской Федерации. Для сведений, составляющих служебную тайну в органах внутренних дел, установлен специальный режим

хранения и доступа. Утрата документов, содержащих такие сведения, либо их разглашение должна предусматривать ответственность в соответствии с Федеральными законами.

Таким образом, только четко сформулированный и юридически закрепленный понятийный аппарат позволит решить проблему распространения информации, составляющей служебную тайну, так как служащие не зная особенностей информации относящейся к этому виду тайны могут распространять ее ни о чем не подозревая. Назрела острая необходимость скорейшего рассмотрения и принятия Федерального закона «О служебной тайне»

Сотникова Я.И.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Применение технических систем разведки и разминирования в борьбе с террористическими угрозами

На сегодняшний день в нашей стране резко обострилась ситуация с терроризмом. Явным примером здесь могут послужить недавние теракты в Волгограде где произошло несколько терактов подряд. Как же действовать спецслужбам при обнаружении взрывчатого вещества и боеприпасов и предотвратить угрозу взрыва. Для этого существуют специальные тактические приемы, а так же технические средства, о них и пройдет речь.

Есть так же более современные наборы. Комплект разведки и разминирования КР95 В-1. Состав:

- Прибор наблюдения ночного ПНН-03М
- Комплект разведки и разминирования КР
- Досмотровое устройство «Перископ-165»
- Устройство локализации взрыва «Ингибитор-1»

- Комплект защитный сапера КЗС
- Жилет транспортный сапера

Но эти наборы используют люди и всегда есть вероятность, что человек может пострадать. В современном мире используются специальные роботы предназначенные для разведки и разминирования.

Например - робот для разминирования "МРК-27Х". Российский робот-сапер, основная задача которого заключается в проведении взрывотехнических работ. Робот способен выполнять различные задачи, среди которых визуальная разведка потенциально опасных для человека зон, поиск, экстренная эвакуация и обезвреживание (уничтожение) различных взрывных устройств.

Дополнительно машина оснащена гидроразрушителями, выносной телекамерой, набором сменных губок, тележкой с небольшим прицепом, а также взрывозащищенным контейнером.

Также, МРК-27Х имеет возможность работать в зонах, характеризующихся повышенным уровнем радиации, обеспечивая разведку, а также укладку радиоактивных элементов в контейнер и их транспортировку.

Кроме того, робот может применяться для проведения операций в условиях химического заражения местности. Он оснащен устройством (спектрометром ионной подвижности), позволяющим делать химический экспресс-анализ воздуха, грунта и жидкостей.
Особенности МРК-27Х:

- относительно небольшие габариты, которые обеспечивают его высокую мобильность за счет возможности доставки к месту проведения операции на легковом автомобиле;
- гусеничное шасси, повышающее проходимость робота по пересеченной местности, лестницам и так далее;
- простая конструкция, что дает возможность адаптировать машину в зависимости от условий заказчика;
- большая грузоподъемность манипулятора, позволяющая работать с грузами до 40 килограмм;
- возможность установки доя восьми камер.

Комплекс МРК-27Х состоит из непосредственно робота-сапера, а также поста дистанционного управления, который состоит из управляющего элемента и двух 10-дюймовых цветных мониторов.

Манипулятор «сапера» способен работать с грузами, массой до 40 килограмм, имеет пять ступеней свободы, а створки раздвигаются на 300 миллиметров.

Роботизированная система разминирования DynaSafe "DynaROVR system 324". Возможности системы - разминирования дистанционно управляемый робот на колёсной базе DynaROVR R30 с подьемным краном и вилами, захватывающее устройство DynaKEEPR G12, защищенная кабина оператора, дистанционное управление на расстоянии до 1 километра, герметичный взрывозащищенный контейнер DynaSEALR X14 с возможностью загрузки до 10 кг взрывчатого вещества в тротловом эквиваленте, трейлер для транспортирования.

DynaROVR system 324 - роботизированная система для безопасного изьятия и транспортировки взрывоопасных предметов, таких как неразорвавшиеся бомбы, мины, снаряды и пр.

Управление осуществляется по радиоканалу на расстоянии до 1 километра из кабины оператора при помощи системы телеНаблюдения. Конструкция крана позволяет поднимать и перемещать предметы весом более 2 тонн. Из кабины оператора возможно управление передвижением робота DynaROVR R30 а также гидравлическим краном, вилами и захватывающим устройством DynaKEEPR G12. Подозрительный предмет захватывается устройством DynaKEEPR G12, перемещается в сторону трейлера, после чего опускается во взрывозащищенный контейнер DynaSEALR X14. Трейлер для перевозки совместим с большинством стандартных автомобилей-тягачей.

Технические характеристики: DynaROVR system 324 - максимальная длина 14,6 м; общий вес 43000 кг.

Робот DynaROVR R30 - радиус дистанционного управления 1000 м; вес 17000 кг; высота (кран в транспортном положении) 3000 мм; ширина (кран в транспортном положении) 2550 мм; длина (кран в транспортном положении) 7200 мм.

Взрывобезопасный контейнер DynaSEALR X14 - допустимая масса взрывчатого вещества 10 кг в тротиловом эквиваленте.

Захватывающее устройство DynaKEEPR G12 - макс. размеры объекта (дхшхв) 900 х 600 х 600 мм; макс. вес объекта 100 кг; мин. размеры объекта (дхшхв) 250 х 250 х 250 мм; мин. вес объекта 1 кг.

Кран - макс. вес объекта 2100 кг; макс. вылет стрелы 12,5 м.

Подъемные вилы - макс. вес объекта 6000 кг; макс. высота подъёма 400 мм.

Многофункциональный мобильный робототехнический комплекс сверхлегкого класса "Вездеход-ТМ5". Многофункциональный мобильный робот сверхлегкого класса МРК "Вездеход-ТМ5" МКРН.461343.003 предназначен для дистанционного выполнения следующих оперативно-тактических задач в труднодоступных и опасных для человека зонах: проведения визуальной разведки с помощью телевизионной системы; поиска и идентификации подозрительных на наличие взрывного устройства (ВУ) предме-тов, расположенных на местности, в зданиях, в салонах или под днищем легковых автотранспортных средств; обезвреживания взрывоопасных устройств с помощью разрушителей "2Р1-У", "2Р4", "Выруб-КМ", "Тайфун"; транспортировки груза в схвате манипулятора и в прицепной тележке; выполнения других технологических операций по обеспечению доступа к ВУ (открывание дверей помещений и автомобилей, замков дверей ключами, выбивание замков с помощью разрушителей). Технические характеристики:

Роботизированный комплекс разведки и разминирования "АЯКС" модель 6211. Предназначен для использования при поиске и обезвреживании взрывоопасных предметов (ВОП) в условиях городской и промышленной застройки. Представляет собой самодвижущееся дистанционно управляемое шасси с комплектом оборудования. Базовая комплектация роботизированного комплекса разведки и разминирования (в дальнейшем -комплекса) включает самодвижущееся шасси, систему дистанционного управления (по радиоканалу), обзорную видеокамеру с системой передачи изображения на видеомонитор, источник ИК-подсветки, лазерный целеуказатель, стрелу-манипулятор с платформой, гнездо для пистолета ПМ с механизмом дистанционного спуска, пульт дистанционного управления, автоматическое зарядное устройство.

Комплекс может быть использован для решения следующих задач:

дистанционный визуальный осмотр в дневных и ночных условиях предметов и помещений с подозрением на наличие в них ВОП;

визуальная идентификация (по возможности) типа ВОП, его взрывателя, массы заряда взрывчатого вещества, наличия или отсутствия осколочного корпуса;

взятие проб воздуха для последующего их анализа на наличие взрывчатых и других веществ;

приведение к срабатыванию оптических взрывателей и взрывателей с натяжными (разбрасываемыми) датчиками цели (растяжками) в помещениях и на открытой местности;

обстрел ВОП из пистолета типа ПМ, багажа с подозрением на наличие в нем таких предметов, замков в дверях помещений и автомашин;

доставка к ВОП различного рода разрушителей ближнего радиуса действия и локализаторов действия взрыва;

закрепление на ВОП и других предметах фала.

Комплекс может быть также использован при задержании и обезвреживании преступников, для дистанционного ведения скрытного аудиовизуального контроля за различными объектами, при проведении поисково-спасательных операций и ликвидации последствий различных аварий.

Малогабаритный колесный мобильный робот для наблюдения и нейтрализации взрывных устройств (сокращенно SON), специально приспособленный к работе в условиях города.

Это дистанционно управляемое, чрезвычайно малогабаритное устройство служит в качестве инструмента наблюдения и обезвреживания подозрительных и, возможно, являющихся взрывными устройствами объектов. Это идеальное средство для ситуаций, когда имеется большая опасность для людей и когда невозможно применять более крупные манипуляторы для нейтрализации взрывных устройств.

Небольшие размеры делают робот идеальным для решения задач в поездах, самолетах, кораблях, офисах и других подобных объектах.

Его высота настолько мала, что он может вкатываться под днище многих типов автомобилей. Его ликвидаторы могут разрушать самые разнообразные взрывные и зажигательные устройства.

Сенсорная система: стандартное оборудование робота представляет собой три весьма чувствительные камеры черно-белого изображения. Камеры направлены вперед, назад и вверх. Это дает

возможность оператору выводить робот из очень узких мест. Камеры можно использовать для осмотра днища автомобиля или пространства под мебелью, например. Для обеспечения лучшего обзора в уже смонтированные держатели в более высокой или более низкой по сравнению с другими камерами позиции можно устанавливать четвертую камеру. Эта камера может также управляться дистанционно. Конечно, эта четвертая камера может быть таким стереоскопической трехмерной камерой которая может создавать пространственное изображение на специальном мониторе. Это особенно важно, если Вы используете SON в качестве "дополнительного глаза", например, при работе с манипуляторами более крупного размера. Камера дает Вам точные изображения с дополнительных точек наблюдения. Рядом с передней камерой находится микрофон с ненаправленными характеристиками. Он обеспечивает дополнительной акустической информацией с места расположения мобильного робота.

Для операций в условиях плохого освещения три стандартные камеры оборудованы светодиодами инфракрасного диапазона. Освещение, не видимое невооруженным человеческим глазом. гарантирует возможность скрытого проведения операций с роботом даже ночью. Светодиоды потребляют очень мало электроэнергии, что позволяет работать с роботом продолжительное время.

Вооружение - устройство имеет два стандартных стреляющих механизма для ликвидаторов взрывных и зажигательных устройств одноразового действия, которые могут выстреливать независимо друг от друга с помощью блока дистанционного управления. Для каждого ликвидатора имеется отдельный лазерный прицел. Это устройство обеспечивает высокую точность попадания при выстреле. Оба ликвидатора и лазерные прицелы установлены на платформе, которая может наклоняться. Это помогает осуществлять прицеливание. Держатели для ликвидаторов можно снимать без применения какого-либо инструмента и заменять их другими для другого вида оружия.

Система вооружения обладает высоким уровнем безопасности. Многоуровневый контроль за безопасностью обеспечивает защиту от случайного срабатывания ликвидаторов. Ликвидаторы могут стрелять вперед и назад. Наклоняя платформу, можно стрелять вверх и вниз.

Титовский Л.Е.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Правовая защита товарного знака

Товарный знак как средство индивидуализации стимулирует потребителя покупать товары определенных производителей. Будучи связующим звеном между изготовителем и покупателем, он способствует оборотоспособности товаров, обеспечивая функцию рекламы. Поэтому исключительное право на товарный знак является весьма уязвимым и часто нарушаемым. Помогают ли нововведения гражданского законодательства - части четвертой ГК РФ - и судебная практика защититься от нарушений прав компаний на хорошо знакомые бренды? Есть ли специфика в оформлении исковых требований правообладателей? Какие инструменты защиты включает административная процедура охраны торговых марок и логотипов?

Защита прав на товарные знаки, которые помогают индивидуализировать товары (работы, услуги) компаний и предпринимателей, может осуществляться как до, так и после регистрации самого знака (логотипа, торговой марки, бренда). Если, например, Роспатент (официальное название - Федеральная служба по интеллектуальной собственности, патентам и товарным знакам) даст вам отказ по заявке о регистрации или признает ее отозванной, то вы вправе подать возражения в Палату по патентным спорам. Срок на обжалование - три месяца со дня получения заявителем такого решения или запрошенных материалов, противопоставленных заявке.

Но все же в любом случае исключительные права на товарный знак появляются у заявителя только после его регистрации. Это, в частности, означает, что отныне никто не вправе использовать без разрешения правообладателя сходные с его товарным

знаком обозначения в отношении товаров, для индивидуализации которых он был зарегистрирован (п. 3 ст. 1484 ГК РФ). Действия по защите нарушенных прав предпринимает сам правообладатель или обладатель лицензии на товарный знак. Его незаконное использование влечет гражданскую, административную или уголовную ответственность.

Защита исключительных прав по общему правилу осуществляется способами, определенными в ст. 1252 ГК РФ. В качестве своих требований заявляйте о прекращении нарушения исключительного права, об изъятии из оборота и уничтожении за счет нарушителя контрафактного товара, этикеток и упаковок и на ваш выбор - о возмещении убытков или выплате компенсации. Последнее наиболее выгодно, так как у вас не будет особых проблем с доказыванием понесенных убытков или упущенной выгоды. Суд рассчитает компенсацию, руководствуясь п. 2 ст. 1515 ГК РФ и своим судейским усмотрением. Ее сумма может составить:

- от 10 тыс. до 5 млн руб.;
- либо двукратный размер стоимости контрафактных товаров;
- либо двукратный размер стоимости права использования товарного знака.

Но прежде всего выясните, какие положения законодательства (с учетом новелл части четвертой ГК РФ) и судебной практики помогут вам обоснованно отстаивать исковые притязания в суде. В частности, когда ваш конкурент использует похожий товарный знак, права на который были им зарегистрированы.

В ст. 1512 ГК РФ перечислены шесть различных оснований для оспаривания и признания недействительным предоставления правовой охраны. Например, можно сослаться на то, что правовая охрана была предоставлена товарному знаку с более поздним приоритетом по отношению к признанному общеизвестным зарегистрированному товарному знаку иного лица. Либо оспаривание может произойти по причине того, что связанные с регистрацией товарного знака действия правообладателя будут признаны злоупотреблением правом или недобросовестной конкуренцией. Кстати, это новелла части четвертой ГК РФ, ранее такого основания не было. Само по себе понятие «злоупотребление правом» открывает более широкие возможности, чем категория «недобросовестная конкуренция».

Законом установлен прямой запрет на регистрацию обозначений, тождественных или сходных до степени смешения с товарными знаками других правообладателей. И вот именно с доказыванием такого тождества (сходства) связано значительное количество споров. Как правило, обозначение считается сходным до степени смешения с другим, если оно ассоциируется с ним в целом, несмотря на отдельные отличия. Сравнение проводится по трем основным критериям: звуковому, графическому и семантическому (смысловому).

Уже складывается судебная практика по вопросам наличия тождества или опасного (до степени смешения) сходства. Речь идет о решениях Палаты по патентным спорам, в которых она отказывает в удовлетворении требований о неправомерности предоставления правовой охраны другому товарному знаку.

Суды, напротив, при разрешении подобных дел учитывают другие критерии и проявляют мало интереса к результатам экспертиз или досудебных заключений, устанавливающих тождество (сходство) знаков. При изучении этих доказательств у судей практически всегда возникает к ним предвзятое отношение. К тому же нередко стороны представляют суду противоположные по своему содержанию результаты экспертных заключений. Этим существенно занижается их доказательственная сила.

Как указал Президиум ВАС РФ в информационном письме от 13.12.2007 № 122 «Обзор практики рассмотрения арбитражными судами дел, связанных с применением законодательства об интеллектуальной собственности», вопрос о степени смешения обозначений является вопросом факта и по общему правилу может быть разрешен судом без назначения экспертизы. Экспертиза в силу ч. 1 ст. 82 АПК РФ назначается, когда для сравнения обозначений требуются специальные знания. Вопрос о сходстве до степени смешения двух словесных обозначений, применяемых на товарах истца и ответчика, может быть разрешен судом с позиции рядового потребителя. Для этого специальных знаний не нужно. Поэтому не спешите ходатайствовать о назначении экспертизы, сэкономьте деньги на дорогостоящих заключениях независимых экспертов.

Суды до сих пор используют в качестве ориентира два июльских решения ВАС РФ за 2006 год. Это, во-первых, поста-

новление Президиума ВАС РФ от 18.07.2006 №2979/06 по делу «Невское» vs. «AMRO Невское». Разрешая этот спор, ВАС РФ указал, что «угроза смешения имеет место, если один товарный знак воспринимается за другой или если потребитель понимает, что речь идет не об одном и том же товарном знаке, но думает, что они оба принадлежат одному и тому же производителю». Такая угроза зависит: 1) от различительной способности знака с более ранним приоритетом, 2) от сходства противопоставляемых знаков и 3) от оценки однородности обозначенных знаком товаров и услуг.

1) для признания сходства товарных знаков достаточно уже самой опасности, а не реального их смешения. Ее наличие может быть установлено исходя, в частности, из результатов соцопросов, представленных правообладателями;

2)необходимо проводить оценку однородности товаров, поскольку она влияет на установление наличия или отсутствия угрозы смешения товарных знаков;

3) наличие серии знаков (т.е. группы товарных знаков одного владельца, имеющих общие элементы) влияет на усиление различительной способности, как, впрочем, и длительность их использования на товарном рынке.

Таким образом, в делах о незаконном использовании товарных знаков суды не ограничиваются формальной оценкой обо значений по сравнительным критериям. Основное внимание они уделяют вопросам восприятия данных обозначений потребителями. Это более объективный и полноценный подход с точки зрения экономических интересов правообладателей.

Угрюмов Д. В.,
аспирант кафедры
Компьютерных технологий
и информационной безопасности
Дорин Н. Е.,
студент 5 курса
Института компьютерных систем
и информационной безопасности

Киберугрозы систем дистанционного банковского обслуживания

Системы дистанционного банковского обслуживания (далее – ДБО) - общий термин для технологий предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (то есть без его визита в банк), чаще всего с использованием компьютерных и телефонных сетей. Для описания технологий ДБО используются различные в ряде случаев пересекающиеся по значению термины: Клиент-Банк, Банк-Клиент, Интернет-Банк, Система ДБО, Электронный банк, Интернет-Банкинг и прочие схожие термины.

Системы ДБО как инструмент снижения операционных расходов, повышения эффективности и конкурентоспособности бизнеса банков получают все более широкое распространение в нашей стране.

В связи с ростом популярности систем ДБО увеличивается и число инцидентов, связанных с работой таких систем.

Атаки на системы ДБО по виду умысла злоумышленника можно разделить на атаки, целью которых является нанесение репутационных потерь, направленных на нарушение нормальной работы системы (прежде всего это относится к атакам типа «отказ в обслуживании»). К перечню злоумышленников с данным мотивом можно отнести террористические и экстремистские группировки, орудующие в информационном пространстве; так называемых «скрипт-киддис», целью которых является нарушение работы информационной системы с личными целями; нечистых на руку конкурентов, стремящиеся помимо репутационных

потерь вызвать также отток клиентов в конкурирующих организациях, в последствии приводящего к снижению экономической прибыли.

Также существуют атаки на системы ДБО с целью получения злоумышленником финансовой выгоды. Как правило данный вид злоумышленников обладает специальными техническими знаниями, в частности имеет глубокие знания об организации локально-вычислительных сетей предприятий, о наличии уязвимостей в системах ДБО, операционных системах и программном обеспечении. Однако, в последнее время наблюдается снижение интеллектуального порога для злоумышленников, приводящего к росту числа инцидентов и сумме нанесенного ущерба.

К числу причин, приводящих к снижению уровня защищенности систем ДБО относятся:

1. Ряд проблем с программным обеспечением, применяемым для работы в системах ДБО.

- Применение нелицензионного программного обеспечения, потенциально содержащее программные закладки;
- Применение устаревшего программного обеспечения, содержащего уязвимости, приводящие к заражению компьютеров, предназначенных для работы с системами ДБО вредоносным программным обеспечением. К их числу относится: устаревшие версии операционных систем, имеющих уязвимости, в последствии используемые злоумышленниками для осуществления несанкционированного доступа к компьютерам, имеющим доступ к системам дистанционного банковского обслуживания; устаревшие версии программного обеспечения «Java» и «AdobeFlash», имеющие большое количество уязвимостей, использование которых приводит к заражению компьютеров, имеющих доступ к системам ДБО;
- Применение некачественного программного обеспечения. Под некачественненным программным обеспечением подразумевается ПО, не соответствующее требованиям информационной безопасности (приводящее к отключению механизмов защиты прямо или косвенно, имеющее в себе недекларированные возможности или приводящее к их возникновению, неоптимизированные решения, приводящие к высокой нагрузке на информаци-

онную систему и приводящее к атакам типа «отказ в обслуживании»). В качестве примера на рисунке 1 приведена выдержка из инструкции одной из популярных систем электронных переводов, для установки и корректной работы которой необходимо отключить один из встроенных механизмов защиты – UserAccountControl (встроенный диспетчер прав доступа, предназначенный для защиты от несанкционированного доступа).

2. Несоблюдение требований информационной безопасности.

Для систем ДБО, функционирующих в финансовых организациях обязательны требования Центрального Банка Российской Федерации (СТ ОБР ИББС).

Федеральным Законом от 27.12.2002 № 184-ФЗ «О техническом регулировании» установлен рекомендательный статус стандартов и иных документов по стандартизации. Однако в соответствии с указанным Федеральным Законом стандарты и иные документы по стандартизации подлежат обязательному исполнению в организациях, если они добровольно принимают решение о присоединении.

Однако на практике требования Комплекса БР ИББС выполняются редко в полном объёме. Связано это с финансовыми и организационными трудностями, предшествующими приведению систему к требованиям вышеуказанного стандарта. Локально-вычислительные сети банковских организаций иногда сконфигурированы неверно на уровне топологии, что может приводить к неверному распределению ролей и прав доступа.

Для коммерческих организаций, не осуществляющих обработку информации, распространение которой не ограничивается Федеральными законами, требования законодательства носят рекомендательный характер. Однако, в виду наличия в таких организациях систем ДБО необходимо применять «лучшие практики» в области информационной безопасности. Таким образом необходимо обеспечивать информационную безопасность систем ДБО не только на стороне кредитно-банковских организаций, но и на стороне клиента (которым может выступать как физическое, так и юридическое лицо). Требования к уровню защищенности, выдвигаемые операторами систем ДБО носят рекомендательный характер и ответственность за их исполнение ложится на плечи организации-клиента.

Следует также отметить и высокий уровень нецелевого использования компьютеров, используемых для осуществления работы с системами ДБО.

3. Сокрытие факта инцидента, связанного с успешными атаками на системы ДБО.

В случае успешной атаки на систему ДБО вне зависимости от мотивов злоумышленника кредитно-финансовая организация несет репутационные , прямые и косвенные экономические потери, не только как провайдер системы ДБО, но и как кредитно-финансовая организация.

В случае, если пострадавшим является организация-клиент системы ДБО, то сумма возможного ущерба может привести к полной остановке деятельности организации в результате оперативно-розыскных мероприятий в связи задержанием средств на расчетном счете организации.

По вышеописанным причинам пострадавшие в результате атаки на систему ДБО организации предпочитают скрывать факт произошедшего инцидента, что приводит к ситуации, когда при возникновении новой угрозы (новых видах и способах осуществления атак, в том числе и использовании новых видов вредоносного программного обеспечения) отсутствует механизм повышения уровня защищенности для их предотвращения.

Для эффективного противодействия атакам на системы ДБО помимо использования современных средств и методов защиты необходимо налаживать более тесное взаимодействие между банками, правоохранительными органами, регуляторами, а также компаниями, работающими на рынке защиты информации с целью снижения времени реагирования на новые угрозы.

Рассмотрим механизм атаки на систему ДБО, в результате которой происходит хищение денежных средств. Для осуществления успешной атаки с использованием вредоносного программного обеспечения злоумышленнику необходимо обеспечить компрометацию ключевой информации, формирование платежного поручения или перевода и сокрытие следов своей деятельности. Ниже рассмотрены способы компрометации ключевой информации

1. Хищение ключей электронной подписи (ЭП) с незащищенных носителей.

Наиболее простая и отработанная технология, при помощи которой до сих пор реализуется большинство атак на клиентов систем ДБО, хранящих ключи ЭП на флешках, дисках, дискетах, в папке на жестком диске и т. д.

2. Хищение закрытых ключей ЭП из оперативной памяти.

По сравнению с первой чуть более сложная атака. Обычно применяется в случае использования клиентом средства защищенного хранения ключей ЭП, которое позволяет извлекать их из закрытой области памяти устройства.

3. Несанкционированный доступ к криптографическим возможностям смарт-карты.

Одна из наиболее опасных и перспективных атак. Реализуется либо при помощи средств удаленного управления компьютером клиента (класса TeamViewer), либо с использованием удаленного подключения к USB-порту (технология USB-over-IP). Ограничением для данной атаки является обязательное подключение смарт-карты (токена) в момент ее проведения.

4. Подмена документа при передаче его на подпись в смарт-карту.

Наиболее сложный и опасный на сегодняшний день вид атак. В данном случае пользователь видит на экране монитора одну информацию, а в смарт-карту на подпись отправляется другая. Параллельно могут быть подменены данные об остатках на счете, выполненных транзакциях и т. д. Также следует отметить, что каждая из четырех перечисленных технологий эффективна не только на своем уровне защиты, но и на всех более «простых».

После формирования платежного поручения злоумышленник осуществляет платежную операцию на имя соучастника, коим может являться как физическое так и юридическое лицо. Как только злоумышленник получает ответ от соучастника о факте успешного перевода денежных средств, внутренним функционалом вредоносного программного обеспечения происходит преднамеренное нарушение нормальной работы операционной системы скомпрометированного компьютера с целью сокрытия результата работы ВПО.

Следует отметить, что подобные атаки совершаются в конце рабочей недели или перед продолжительными праздниками с целью увеличить период обнаружения и, как следствие, момент

начала реагирования на произошедший инцидент. Поэтому специалисты настоятельно рекомендуют сотрудникам, ответственным за работу с такими финансовыми системами, быть особенно внимательными в подобные периоды и чаще проверять выписки по платежным поручениям.

Внимание стоит уделить нецелевому использованию компьютеров, имеющих возможность перевода денежных средств. Необходимо свести к минимуму функциональное предназначение таких машин, жестко зафиксировать список необходимого для работы программного обеспечения, выход в интернет осуществлять только по «белым спискам», регулярно обновлять антивирусное, прикладное программное обеспечение и операционные системы.

Фархатов Р.Б.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Цимбал В.Н.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Антитеррористические средства и системы

Серьезной проблемой последнего десятилетия XX века – начала XXI века, влияющей на состояние общества, негативно сказывающейся на общественном порядке, вызывающая рост преступности является террористическая деятельность.

Под терроризмом (от латинского «terror» - страх, ужас) понимается физическое насилие по отношению к политическим противникам вплоть до их уничтожения, а террористами называют участников различных актов индивидуального или иного террора. Объективно терроризм представляет собой сложное явле-

ние, посягающее на те, или иные, охраняемые законом сферы жизнедеятельности людей различным способами[1].

В Российском законодательстве, а именно в п. 1 ст. 3 ФЗ «О противодействии терроризму» от 06.03.2006 № 35-ФЗ под терроризмом понимается: «Идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий».

Но терроризм, в свою очередь, проявляется в виде различных действий или деятельностью, то есть террористической, которая в соответствии с п. 2 той же статьи вышеуказанного ФЗ включает в себя:

а) организацию, планирование, подготовку, финансирование и реализацию террористического акта;

б) подстрекательство к террористическому акту;

в) организацию незаконного вооруженного формирования, преступного сообщества (преступной организации), организованной группы для реализации террористического акта, а равно участие в такой структуре;

г) вербовку, вооружение, обучение и использование террористов;

д) информационное или иное пособничество в планировании, подготовке или реализации террористического акта;

е) пропаганду идей терроризма, распространение материалов и информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности.

Правовую основу противодействия терроризму составляет Конституция Российской Федерации, общепринятые принципы и норма международного права, международные договоры Российской Федерации, указанный выше ФЗ от 06.03.2006 № 35-ФЗ и иные федеральные законы, нормативно-правовые акты Президента Российской Федерации, нормативно-правовые акты Правительства Российской Федерации, а также принимаемые в соот-

[1]См.: Смиртин А.Н. Экстремизм и терроризм: некоторые подходы к определению понятий // Вестник Санкт-Петербургского университета МВД России. – Вып. 1 (49), 2009. – С. 55.

ветствии с ними нормативные правовые акты других федеральных органов государственной власти.

Министерство внутренних дел России осуществляет борьбу с терроризмом посредством предупреждения, выявления и пресечения преступлений террористического характера, преследующих корыстные цели. Через Национальное центральное бюро Интерпола в соответствии с возложенными на него функциями осуществляет взаимодействие между различными государствами по розыску и привлечению к уголовной ответственности лиц, обвиняемых в терроризме[1].

Основной формой пресечения террористического акта является контртеррористическая операция, которая предусматривает «Реализацию комплекса специальных, оперативно-боевых, войсковых и иных мероприятий с применением боевой техники, оружия и специальных средств по пресечению террористического акта, обезвреживанию террористов, обеспечению безопасности граждан, организаций и учреждений, а также по минимизации и (или) ликвидации последствий проявлений терроризма»[2].

Если рассмотреть статистику совершения террористических актов, то в докладе Национального консорциума по изучению терроризма и ответов на терроризм при Мэрилендском университете США отмечается, что в 2012 году 8500 террористических актов по всему миру унесли жизни почти 15,5 тыс. человек. 2012 г. – рекордный по числу терактов и количеству жертв. Наблюдения ведутся с 1970 года. Исследователи отмечают, что большая часть терактов совершалась в тех странах, где доминирует мусульманское население[3].

Борьба с терроризмом невозможна без оснащения соответствующих служб и структур, отвечающих за безопасность общества, эффективными техническими средствами дистанционного обнаружения скрытых в различных объектах оружия, взрывных

---

[1]См.: Административная деятельность органов внутренних дел. Часть Особенная. Учебник. - М.: МЮИ МВД России. - Издательство «Щит-М», 1997.

[2]См.: ст. 23 Концепции противодействия терроризму в Российской Федерации (утв. Президентом РФ от 05.10.2009).

[3]Википедия. Свободная энциклопедия. URL: http:\\ru.wikipedia.org/wiki / Терроризм (дата обращения: 07.01.2014).

устройств, взрывчатых, наркотических, отравляющих и радиоактивных веществ.

К антитеррористическим средствам и системам относятся следующие группы поисковых устройств:

– средства визуального контроля;
– металлоискатели;
– рентгено-просмотровая техника;
– газоанализаторы;
– обнаружители оптических устройств;
– детекторы состава веществ, основанные на ядерно-физических методах (нейтронный, фотоядерный, ядерно-магнитного и ядерно-квадрупольного резонансов и др.);
– нелинейные радиолокаторы;
– обнаружители приемников радиоуправляемых взрывных устройств;
– обнаружители временных замедлителей взрывных устройств;
– беспилотные летательные аппараты.

К средствам нейтрализации террористических угроз можно отнести следующие технические устройства:

– роботизированная техника;
– постановщики радиопомех, используемые при работе с подозрительными предметами;
– разрушители подозрительных предметов;
– локализаторы подозрительных предметов;
– взрывозащитные средства.

Современный терроризм характеризуется резко возросшей технической оснащенностью, высоким уровнем организации, наличием значительных финансовых средств. Его главная отличительная черта - это размывание границ между международным и внутренним терроризмом. Расширяются связи террористических организаций с наркобизнесом и незаконной торговлей оружием. Заметна динамика роста террористических групп в современном мире.

Для обеспечения необходимой эффективности борьбы с терроризмом требуется одновременное целенаправленное воздействие на социальные факторы и условия, которые детермини-

руют терроризм и благоприятствуют его распространению. В решении задач, предназначенных для осуществления социальной, криминологической и специальной профилактики, должен участвовать широкий круг государственных органов с привлечением общественности.

В целом мероприятия по противодействию терроризму должны включать в себя:

– идеологическое, информационное, организационное противодействие формированию у граждан террористических намерений и настроений;

– правовое, информационное, административное и оперативное противодействие возникновению террористических (экстремистских) групп и организаций;

– недопущение приобретения оружия, боеприпасов и иных средств осуществления преступных действий лицами, вынашивающими замыслы на совершение террористических актов;

– предупреждение террористических действий на стадии их подготовки и совершения;

– оперативное, боевое, техническое, уголовно-правовое пресечение террористических действии на стадии их реализации.

Все перечисленные выше устройства позволяют выявить и нейтрализовать террористические угрозы при определенных условиях. Реальная эффективность использования технических средств зависит от существующей технологии контроля и квалификации персонала, их использующего. Технические средства, в основном, позволяют получить вспомогательную информацию, необходимую для принятия решения лицам, осуществляющим руководство конкретными антитеррористическими мероприятиями.

Фурсова Ю.М.,
студент института информационных
технологий и безопасности
Куб ГТУ

Анализ состояния защиты информации от внутренних утечек (по материалам отечественной и мировой печати)

Последний год ознаменовался многими громкими событиями в области информационной безопасности. Среди них одним из особо впечатляющих можно назвать атаки китайских хакеров на известные американские IT-компании, в том числе Twitter, Facebook, Apple и Microsoft. Также стоит отметить крупнейшую чуть ли не за всю историю интернета DDoS-атаку на серверы компании Spamhaus. Не осталась без внимания общественности история, связанная с именем Сноудена, разоблачившего действия Агенства Национальной Безопасности США, представив широкой огласке сведения о слежке за информационными коммуникациями между гражданами многих стран мира.

Как видно из этих немногих примеров, всего лишь за один год безопасность данных пользователей, организаций и компаний очень часто становилась под угрозой. Поэтому можно с уверенностью утверждать, что проблема защиты информации продолжает оставаться актуальной.

Согласно исследованию в области утечек конфиденциальной информации , проводимому ГК «Infowatch» с 2008 года, в первом полугодии 2013 года было зафиксировано 496 случаев утечки информации. Большая часть утечек приходится на персональные данные – 93,8%. Причем, 67% приходится на коммерческие организации, и около 30% - государственные структуры. При этом количество неопределенных источников утечки сократилось до 3%. Это относится и к России, где к 2011 году ужесточили требования к операторам баз данных, внеся поправки в Федеральный закон «О персональных данных».

Почти в половине случаев утечка произошла умышленно, следовательно, утечка конфиденциальной информации не всегда явля-

ется злонамеренным действием и не стоит забывать о пресловутом человеческом факторе при разработке концепций политики ИБ.

Такие сведения свидетельствуют о крайней ликвидности персональных данных (ПДн) и стабильной популярности у злоумышленников. В то же время можно утверждать, что общий уровень защиты данных крайне низок. Коммерческие и государственные организации готовы раскрывать факт утечки и проводить исследования инцидентов, но не проводят эффективных мер для предотвращения утечек ПДн.

Следующими по количеству утечек являются коммерческая тайна или конфиденциальные сведения, связанные с коммерческой деятельностью – 3,4%. Так как утечка данного характера полностью сказывается на финансовом положении компаний любого размера, то для них вопрос о защите секретов производства встает наиболее остро.

Количество утечек государственной тайны сравнительно мало, возможно, по причине низкой огласки, возможно, в связи с более совершенной нормативно-правовой базой, и как следствие, лучшими методологиями по обеспечению безопасности информации.

Тем не менее, сведения, содержащие государственную и коммерческую тайну, остаются под угрозой осуществления несанкционированного доступа извне.

Согласно отчету Kaspersky Security Bulletin за 2013 год [2] остаются популярными атаки, связанные с кражей данных государственных, ведомственных и муниципальных учреждений различных стран, а также крупных промышленных, отраслевых компаний (атака Winnti), СМИ. Такие атаки приобрели целевой характер и организовывались профессиональными группировками, в том числе наёмными (IceFog), занимающимися кибершпионажем.

Стремительный прогресс в области ИТ привел к активной компьютеризации бизнес-процессов. Поэтому, помимо государственных учреждений, жертвами краж данных становились и коммерческие организации. Целью атак в данном случае становилось хищение и уничтожение ценной информации, кража денежных средств и нанесение финансового ущерба, вследствие падения доверия к компании. Зачастую злоумышленники действуют также целенаправленно и планомерно, предварительно собрав и изучив всю необходимую информацию о компании.

Атакующие прибегают к таким методам, как использование уязвимостей приложений, атаки компьютера посредством скачивания пользователем зараженного ПО и использование бэкдоров.

Как и раньше, одним из ключевых является человеческий фактор. Зная о неграмотности подавляющего большинства пользователей в вопросах ИБ, злоумышленники прибегают к методам социальной инженерии, чтобы собирать данные об организации, ее сотрудниках и другую информацию, необходимую для проведения успешной атаки. Стоит учитывать, что зачастую хакеры получают возможность провести даже несложную атаку как раз благодаря неосведомленности пользователей и сотрудников в вопросах безопасного поведения в сети.

Со стремительной интеграцией Интернета в нашу жизнь связано развитие систем электронных платежей, интернет-банкинга, а также электронного маркетинга. Все это является плацдармом для создания вредоносного ПО, целью которого является кража паролей и логинов пользователей, вымогательство (Cryptolocker).

С развитием мобильных технологий и популяризацией мобильных приложений под угрозой оказались данные пользователей, хранящиеся на смартфонах и других мобильных устройствах. Особенно уязвимы устройства на базе Android, для которых за последний год было обнаружено почти 98% вирусных приложений из всего вредоносного ПО для мобильных телефонов, в том числе мобильные ботнеты, троянцы, бэкдоры. Данная операционная система (ОС) пользуется такой большой популярностью у злоумышленников по ряду причин: ее распространенность, открытость ресурсов, возможность отслеживать пользователей, необходимость разрешения доступа к широкому набору данных для успешной работы.

Помимо того, на практике оказывается, что мобильное вредоносное ПО более стабильно по сравнению со зловредами, предназначенными для персональных компьютеров (ПК). Осуществить заражение на смартфонах с целью кражи денег или спам-рассылки, управлять зараженным устройством через интернет, посылая ему инструкции, или с помощью мобильных ботнетов вероятнее, потому как смартфон включен в сеть, даже в том случае, если пользователь не взаимодействует с ним.

Атакующие активно используют уязвимости известных легитимных приложений (OracleJava, Windows приложения), которые наиболее популярны у пользователей, для заражения через интернет-ресурсы. Согласно отчету, за 2013 год количество атак с веб-ресурсов увеличилось почти в 1,2 раза. Угроза осуществление атак данного вида возрастает из-за игнорирования пользователями обновлений, предоставляемым разработчиками.

Распространение кросс-платформерного программного обеспечения дает злоумышленникам больший простор для их деятельности: это позволяет разрабатывать вредоносные приложения для различных ОС и платформ, используя эксплойты одних и тех же, в том числе популярных (Java, Adobe), программ.

В дальнейшем, предполагают авторы отчета, следует ожидать динамику в развитии вредоносного ПО для мобильных устройств, учащение атак на облачные хранилища данных в связи с огромным количеством информации на них, а также популяризации услуг кибернаемников.

Эти опасения подтверждаются авторами издания по безопасности от Cisco , где говорится об увеличении глобального облачного трафика, развитии «Всеобъемлющего интернета», объединяющего разрозненные данные пользователей, и росте взаимодействия между ними.

Уже сейчас можно утверждать об увеличении мобильного трафика, популярности подключение к ресурсам интернета через планшетные ПК и смартфоны. В будущем эта тенденция только усилится, количество устройств, подключаемых к сети, будет только расти, поэтому стоит задуматься об обеспечении безопасности информации, хранящейся на отдельных устройствах, но объединенных с помощью глобального расширяющегося киперпространства.

Стойкое увеличение массива данных предполагает такое же стремительное развитие облачных вычислений и облачных хранилищ данных. Глобальный облачный трафик, по подсчетам аналитиков Cisco, в следующие пять лет может увеличиться вшестеро. Поэтому стоит задаться вопросом о возможности правильной организации столь большого количества данных.

Таким образом, авторы отчета объединили информационные массивы мобильных устройств и облачных хранилищ в одну

высокотехнологичную среду, созданную под эгидой концепции Всеобъемлющего интернетом.

Также на сегодняшний день наиболее актуальным становится вопрос об изменении понимания безопасности информации в вопросе анонимности. По этому поводу стоит отметить, что сейчас можно столкнуться с двумя диаметрально противоположными мнениями.

В первом случае говорят о снижении анонимности в сети. Наиболее наглядно эта проблема рассматривается на примере пользования криптовалютой Bitcoin. Банк России, к примеру, утверждает, что анонимность виртуальных валют и доступ к ним неограниченного числа пользователей способствует направлению легализации средств, добытых преступных путем, а также возможности, в том числе непреднамеренно, участвовать в противоправной деятельности злоумышленников. Известны примеры, когда преступные группировки использовали Bitcoin для проведения своей деятельности, например случай с сайтом Silkroad, организовавший подпольную продажу наркотической продукции.

С другой стороны, в связи с распространением в СМИ сведений о массовой слежке за гражданами через сети, стоит задуматься об ограничении использования идентификаторов пользователей сети, если это каким-то образом ведет к посягательству на их частную жизнь.

Представив сложившуюся картину в ИБ, можно заметить назревающие сложности в этой области. Из-за увеличивающегося массива данных, возможно, будет необходимо посмотреть на безопасность пользовательских данных с другой стороны, изменить существующие концепции в применении средств и методов. К примеру, использование межсетевых экранов в условиях облачных технологий не сможет обеспечить защиту в полной мере.

Новые тенденции в сфере угроз ИБ должны привлечь многих специалистов, каким-либо образом связывающих свою деятельность с информационными коммуникациями, для реализации комплексного подхода в анализе угроз и методов их предотвращения.

В заключение хочется добавить, что по причине роста числа угроз и изменения их характера стоит обратить внимание не только специалистов в области ИТ, но и самих пользователей на эту проблему.

Хохлов Н. М.,
курсант филиала Военной академии связи им. Буденного
научный руководитель:
Чернуха Ю. В.,
кандидат технических наук,
доцент кафедры
филиала Военной академии связи им. Буденного

Задача оптимизации состава программно-технического комплекса защиты информации

Высочайшая степень информатизации, к которой стремятся Вооруженные силы Российской Федерации, ставит эффективность их использования в зависимость от защищенности информационных технологий, обеспечивающих выполнение ими своего функционального предназначения. Сегодня, применяемые в ВС РФ компьютерные системы и телекоммуникации во многом определяют надежность систем обороны и безопасности страны, обеспечивая хранение конфиденциальной информации, ее обработку, доставку и представление.

Острота проблемы обеспечения безопасности информационных отношений в Вооруженных силах, при применении новых информационных технологий, вызвана, прежде всего, расширением сферы применения в различных структурах Вооруженных сил компьютерной техники и возросшим уровнем доверия к новым информационным технологиям, формирующим и обрабатывающим электронные документы, содержащие сведения ограниченного доступа (конфиденциального характера).

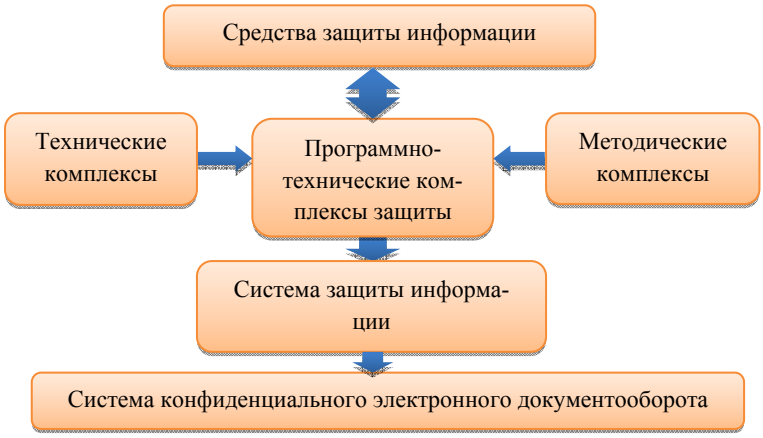
В статье представлены результаты анализа актуальности исследования в рамках военно-научной работы «Структура-11», выполняемой на кафедре Криптографических средств защиты информации и математических основ криптологии Филиала военной академии связи (г. Краснодар)

Понятие «внедрение новых информационных технологий в военное дело» определяет круг организационно-технических вопросов, связанных с созданием современных средств вооруженной борьбы и систем, обеспечивающих их эффективное примене-

ние, за счет совершенствования процессов сбора, хранения, передачи и обработки информации с помощью современных средств вычислительной техники и программного обеспечения.

По прогнозам, уже к 2020 г. только около 5% информационных ресурсов по вопросам жизнедеятельности войск и сил флота останется в бумажном виде, а 95% информации будет храниться в электронном виде.

Таким образом, в современных условиях вследствие интенсивного развития современных информационных технологий и средств телекоммуникаций, на передний план при проектировании и создании систем конфиденциального электронного документооборота (СКЭД) выходит задача построения эффективных систем защиты информации.



Системы защиты информации (СЗИ), интегрируются в СКЭД в качестве проблемно – ориентированных подсистем. При этом сами СЗИ являются сложными организационно-техническими системами, которые включают в свой состав объекты защиты, органы и исполнителей с используемыми ими техникой и способами защиты информации.

Основой таких систем служат программно-технические комплексы защиты информации (ПТКЗИ), объединяющие взаимосвязанную совокупность различных программных и технических средств защиты информации (СрЗИ).

Как объект проектирования ПТКЗИ, являющийся базовой структурной составляющей СЗИ, представляет собой сложный технический объект, включающий различные технические и программные подсистемы и элементы, объединенные в программно-технические комплексы (ПТК) и программно-методические комплексы (ПМК), и характеризуются большим количеством разнородных параметров.

При разработке ПТКЗИ требуется решать два типа задач:

осуществить синтез (структурный и параметрический) проектируемого комплекса в рамках возможных угроз и каналов утечки информации;

провести анализ его эффективности в процессе функционирования с целью выбора наиболее эффективных в заданных условиях способов и средств защиты информации.

При этом решение таких задач осложняется тем, что для каждого структурного элемента ПТКЗИ и выполняемой функции возможно применение различных программных и технических средств, во множестве представленных на рынке.

Следовательно, повышение эффективности процесса разработки систем защиты информации может быть достигнуто за счет совершенствования существующих и разработки новых алгоритмов, охватывающих различные задачи и этапы данного процесса, которые должны основываться на создании соответствующего математического обеспечения (МО) и реализовываться в программном обеспечении, что позволит повысить качество и автоматизировать основные этапы проектных работ.

Такие алгоритмы должны охватывать и техническую, и программную стороны формируемых ПТКЗИ, учитывать многоэтапность его разработки, включать в себя целый ряд процедур синтеза и анализа, характерных как для разработки различных ПМК и ПТК, так и учитывающих специфику СЗИ.

Одной из важнейших таких задач является выбор из множества имеющихся сертифицированных средств защиты информации таких, которые позволяют получить наиболее рациональную структуру и в ее рамках сформировать состав конкретного ПТКЗИ, обеспечивающего перекрытие всех выявленных каналов утечки и несанкционированного доступа (НСД) с заданной эффективностью.

Анализ принципов эволюционного развития защищенных информационных технологий показывает, что на каждом его этапе состав и характеристики используемых средств защиты информации определялись на основании личного опыта разработчиков, с учетом существующей и рекомендуемой к применению номенклатуры программных и аппаратных средств. Данное обстоятельство противоречит принципам системного подхода к проектированию защищенных информационных технологий, в

соответствии с которыми все функции должны быть связаны в единый технологический процесс и основываться на общих моделях реализации .

Анализ содержания этапов разработки ПТКЗИ и входящих в них процедур позволяет сделать вывод, что они содержат задачи как слабоформализуемые, требующие для выполнения квалифицированных специалистов, привлечения экспертов, применения эвристических методов и подходов, так и такие, которые могут быть формализованы в рамках задач и методов структурного синтеза с привлечением положений теории математического программирования (формирование структуры ПТКЗИ, оптимальный выбор состава средств защиты), а также на основе методов математического моделирования случайных процессов и систем (расчет, оценка и анализ показателей эффективности СрЗИ и ПТКЗИ в целом).

Используемые в настоящее время подходы к построению алгоритмического обеспечения для решения рассмотренных задач, имеющиеся алгоритмы не носят комплексного характера, недостаточно учитывают взаимосвязь и взаимозависимость частных задач, не уделяют достаточного внимания вопросам оптимальности формирования и выбора наиболее рациональных вариантов ПТКЗИ с учетом требуемых значений показателей эффективности.

Общим недостатком многих работ, особенно рассматривающих задачу создания СЗИ в формальной постановке, является недостаточное применение в целевых функциях и ограничениях основного показателя эффективности, связанного с вероятностными характеристиками функционирования СрЗИ и ПТКЗИ в целом.

В настоящее время исследования задачи обеспечения требуемого уровня защищенности систем конфиденциального электронного документооборота (СКЭД) ведутся, как в направлении раскрытия природы явления, заключающегося в нарушении целостности и конфиденциальности информации, дезорганизации работы системы в целом и ее элементов в частности, так и в направлении разработки конкретных практических методов и средств их защиты. Серьезно изучается статистика нарушений, вызывающие их причины, суть применяемых противником приемов и средств, используемые при этом недостатки систем и

средств их защиты, обстоятельства, при которых было выявлено нарушение, и другие вопросы.

Необходимость применения систем электронного документооборота, при решении задач военного управления, становится еще более актуальной в связи с развитием и распространением в видах и родах ВС РФ территориально-распределенных систем и систем с удаленным доступом к совместно используемым ресурсам, что закономерно приводит к необходимости постоянного совершенствования, в том числе и алгоритмов синтеза оптимальной структуры и состава ПТКЗИ.

Таким образом, задача развития алгоритмического обеспечения процедур формирования рациональной структуры, оптимального выбора состава СрЗИ при проектировании СЗИ в СКЭД является весьма актуальной.

Литература:

1. Чернуха Ю.В. Обеспечение информационной безопасности систем защищенного электронного документооборота/ Краснодар: ООО Империя Печати, 2013.-139 с.

Чернуха Ю. В.,
кандидат технических наук,
доцент кафедры
филиала Военной академии связи им. Буденного

Некоторые аспекты защиты персональных данных

27 июля 2006 года Президент РФ В. В. Путин подписал закон N152-ФЗ «О персональных данных». В сферу действия этого нормативного акта попадают все юридические и физические лица, на попечении которых находятся приватные сведения других граждан. Новый закон требует, чтобы каждая организация, владеющая персональными данными своих сотрудников, клиентов, партнеров и т.д., обеспечила из защиту. В случае нарушения положений закона компания может лишиться лицензии и подвергнуться судебному преследованию со стороны граждан, чьи приватные записи были скомпрометированы. Кроме того, виновные

лица, нарушившие требования закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

В данной статье в виде тезисов рассмотрены некоторые аспекты деятельности по защите персональных данных, а также основные недостатки, выявленные при проверке выполнения требований законодательства по защите персональных данных при реализации мер технического характера.

1. В настоящее время существуют много стратегий на основании которых можно построить систему защиты информации это в первую очередь стратегии на основе анализа рисков (построения модели угроз) и на основе анализа детерминированных требований (РД ФСТЭК).

2. Сложность начальных этапов создания системы защиты ПДн на предприятии (организации) в основном обусловлена наличием различного рода недочетов, и это подтверждают эксперты, которые, хоть и в меньшей степени, к сожалению пока присутствуют в нормативно-правовой базе предназначенной для решения проблемы защиты персональных данных, начиная с терминологии и заканчивая различным процедурными вопросами.

3. Чтобы правильно и полно заполнить Уведомление необходима комплексная работа (кадровик, бухгалтер, специалист ИТ).

4. Надо очень хорошо знать законодательство в своей сфере работы, чтобы максимально точно определить какие категории ПДн обрабатываются надо ли получать согласие или эти данные предоставляются в соответствии с федеральным законом.

5. Если вы коммерческая организация и не знаете что делать, то смотрите требования для государственных – лишним не будет.

6. Только один документ имеет строгую форму и требования к заполнению - УВЕДОМЛЕНИЕ (приказ № 706 от 2011 года)

Для СОГЛАСИЯ, запросов и ответов определено только содержание, но не определена форма представления (решение принимает оператор)

Журналы, инструкции и т.д. разрабатываются в соответствии с рекомендациями РНК, ФСТЭК и ФСБ.

7. Чем полнее перечислены категории персональных данных и цели обработки, на которые дается ПИСЬМЕННОЕ

СОГЛАСИЕ, тем спокойнее в первую очередь ОПЕРАТОРУ, а не субъекту персональных данных.

8. Документы определяющие требования по защите ПДн составляются не в интересах Роскомнадзора, ФСБ ли ФСТЭК, а в интересах самого оператора для того чтобы в случае проблем с ПДн было чем доказывать свою состоятельность в этом вопросе. А если документов нет, то и доказывать ничего не надо – ВИНОВАТ.

9. Все документы организации, предназначенные для внесения в них конфиденциальной информации (персональных данных) вводятся приказом руководителя. Не вводятся только те документы, которые предусмотрены законодательными актами. Например: не надо вводить приказом форму Т-2, так как она предусмотрена законодательством.

10. Во всех типовых документах организации должна иметься информация о том чем (кем) узаконен этот документ (т.е. на каком основании разработан или кем введен в действие).

11. В интернете в блогах можно встретить много рекомендаций по различным вопросам защиты ПДн в любых сферах. Однако к этим рекомендациям тоже надо относится, с некой долей скептицизма. Все дело в том, что многие блоггеры не всегда имеют достаточную подготовку в области информационной безопасности и поэтому их рекомендации носят субъективный характер, не всегда основываются на всем перечне руководящих документов, практиках проверок и судебной практике в области защиты персональных данных. А в планах некоторых семинаров присутствуют такие заявления: «Вы научитесь строить систему защиты ИСПДн» и это за 4 часа обсуждения.

Среди основных недостатков, выявленных при проверке выполнения требований законодательства по защите персональных данных при реализации мер технического характера можно отметить следующие:

1. Отсутствие требований по технической защите персональных данных в техническом задании и проектной документации (в соответствии с СТР-К). В негосударственных организациях документации на систему защиты ПДн, как правило, нет вообще.

2. Незавершенность классификации ИСПДн или ее ошибочность.

3. Невыполнение работ по анализу угроз информационной безопасности. Непонимание методики составление частной модели угроз (методрекомендации ФСТЭК почти никто не читает, копируют модель из Интернета не замечая грубых ошибок).

4. Несоответствие применяемых средств модели угроз.

5. Незавершенность разработки необходимого комплекта организационно-распорядительной документации (скачивают документы с Интернет, не проводя никакого анализа на соответствие реальному положению дел).

6. Нарушение требований основных положений приказа № 21 ФСТЭК в плане построения подсистем защиты ПДн и как результат отсутствие необходимых (требуемых) мер и сервисов защиты информации.

7. Отсутствие правил работы (использования, применения) средств защиты информации, применяемые для защиты ПДн.

8. Непринятие мер по учету машинных носителей.

9. Отсутствие в должностных регламентах ответственных лиц за защиту персональных данных и их полномочий по контролю за выполнением требований по защите.

10. Отсутствие достаточного количества квалифицированных специалистов.

В заключении необходимо отметить. что самая главная проблема построения системы защиты персональных данных заключается в том, что адекватно-критериально оценить правильность решения этой задачи не всегда могут даже регуляторы. Так как многие документы разработанные «в верхах», к сожалению, остаются непонятными, как тем кто их должен исполнять, так и тем кто должен контролировать их исполнение.

Другими словами несовершенство или сложность понимания нормативной базы позволяет одно и тоже решение по построению системы защиты считать, как правильным, так и ошибочным. И борьба начинается уже не на нормативно-техническом, а на юридическом уровне. Но при обоюдно адекватном подходе к решению задачи защиты персональных данных оператора и регулятора всегда можно найти компромисс, вся проблема в том, что этого компромисса можно не достичь с субъектом ПДн, права которого нарушены. Поэтому знание и главное понимание нормативно-правовой базы шанс доказать свою правоту.

Чикида В.И.,
курсант 2 курса
Краснодарского университета МВД России
научный руководитель:
Сизоненко А.Б.,
начальник кафедры ИБ
Краснодарского университета МВД России

Анализ уязвимостей систем документооборота органа внутренних дел

Документооборот, является неотъемлемой и важной частью функционирования любой организации. В соответствии с ГОСТ 51141-98 «Делопроизводство и архивное дело. Термины и определения» документооборот – это движение документов в организации с момента их создания или получения до завершения исполнения или отправления.

Следует отметить, что в этом определении упор делается на «движении документов», которое осуществляется посредством выполнения ряда делопроизводственных операций, образующих следующие стадии документооборота: прием и первоначальная обработка документов (корреспонденции), исполнение документов, отправка корреспонденции, хранение документов. К примеру, в органах внутренних дел документы адресуются руководителю органа внутренних дел, который назначает исполнителя. Таким образом, путь движения документа будет многоступенчатым сверху вниз. Отсюда следует, что документооборот зависит от системы управления, он вторичен по отношению к ней, но в то же время именно документооборот, отражая систему управления, позволяет ее наглядно увидеть.

Несмотря на вторичность порядка движения документов по отношению к целям и задачам организации, документооборот рекомендуется нормировать и регулировать. В технологической цепочке обработки и движения документов выделяются этапы:

– прием и первичная обработка поступающих в организацию документов;

– предварительное рассмотрение и распределение документов;

– регистрация документов;

– контроль за исполнением;

– исполнение документов, их составление, согласование, оформление;

– отправка или направление в дело.

Основополагающим объектом исследования и совершенствования можно назвать документопоток.

Документопоток – это поток документов, циркулирующих между пунктами обработки и создания информации (руководителями организации и структурных подразделений, специалистами) и пунктами технической обработки документов: экспедицией, секретариатом, канцелярией, копировально-множительной службой и др.

Содержание документопотока характеризуется составом документов, входящих в него, и составом информации, закрепленной в этих документах.

Структура документопотока описывается признаками, в соответствии с которыми может быть осуществлена классификация документов и их индексация, сформирована система научно-справочного аппарата по документам организации. В значительной степени структура документопотоков соответствует функционально-целевому назначению составляющих его документов.

Количество документов всех потоков, независимо от способа создания, получения (доставки), т.е. включая факс, электронную почту, доставку курьером или посетителем, составит суммарный объем документооборота организации

Теперь разберем понятие уязвимости. В ГОСТ 50922-2006 дано следующее определение: уязвимость – это свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Уязвимость любой информации заключается в нарушении ее физической сохранности вообще либо у данного собственника (в полном или частичном объеме), структурной целостности, доступности для правомочных пользователей. Уязвимость информации конфиденциального характера, в том числе

составляющей государственную тайну, дополнительно включает в себя нарушение ее конфиденциальности.

Возможность изменения или нарушения действующего статуса информации обусловлено в первую очередь ее уязвимостью, которая означает неспособность информации самостоятельно противостоять дестабилизирующим воздействиям, сохранять при таких воздействиях свой статус. Но уязвимость информации не существует как самостоятельное явление, а проявляется (выражается) в различных формах. К формам проявления уязвимости систем документооборота, выражающим результат дестабилизирующего воздействия на информацию, могут быть отнесены:

– хищение носителя информации или отображенной в нем информации;

– потеря носителя информации;

– несанкционированное уничтожение носителя или отображения в нем информации;

– искажене информации;

– блокирование информации;

– разглашение информации.

Анализ уязвимости необходимый этап в создании эффективной системы защиты документированной информации. По результатам анализа уязвимостей могут быть разработаны защищенные системы документооборота. Причем понятие «защищенные» должно отражать не только обеспечение конфиденциальности систем документооборота, но и целостности и доступности.

Шамханов Т.С.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Средства поиска взрывных устройств

В настоящее время террористические акты в различных странах мира с применением взрывных устройств требуют усиления борьбы с терроризмом и постоянного совершенствования средств поиска взрывных устройств.

Демаскирующие признаки взрывного устройства обусловлены главным образом следующими факторами:

- наличием взрывчатых веществ в конструкции взрывного устройства;
- наличием антенны с радиоприемным устройством у радиоуправляемого взрывного устройства;
- наличием часового механизма или электронного таймера (временного взрывателя);
- наличием проводной линии управления;
- наличием локально расположенной массы металла;
- неоднородностями вмещающей среды (нарушение поверхности грунта, дорожного покрытия, стены здания, нарушение цвета растительности или снежного покрова и т.д.);
- наличием теплового контраста между местом установки и окружающим фоном;
- характерной формой взрывного устройства.

Взрывное устройство содержит как правило от нескольких десятков граммов до нескольких килограммов взрывчатого вещества. Поэтому взрывное устройства в принципе можно обнаружить путем регистрации газообразных испарений продуктов медленного разложения или испарения взрывчатого вещества. Регистрация может осуществляться с помощью химического, масс-спектрометрического и других способов. Концентрация паров

взрывчатых веществ достигает 10-7 - 10-8 г/л у поверхности грунта над местом установки противотанковой мины (при положительной температуре), находящейся на глубине 5 см. Вблизи взрывного устройства без маскирующего слоя концентрация паров взрывчатого вещества может быть на несколько порядков выше.

Химический способ обнаружения взрывчатого вещества реализуется в аэрозольных тестах. Например, отечественный комплект аэрозолей "Expray" (ОСТ-731) позволяет обнаружить практически все виды взрывчатых веществ (тротил, тетрил, динамит, нитроглицерин, нитроцеллюлозу, оксид пикрина). Наличие того или иного цвета, который проявляется на тестовой бумаге, позволяет доказать, что в проверяемом объекте (кейсе, коробке, письме) находится взрывчатое вещество. Проведение полного теста занимает не более минуты.

Следует отметить, что в настоящее время лучшим детектором взрывчатых веществ является собачий нос. Специально обученные собаки минно-розыскной службы способны избирательно обнаруживать весьма малые количества взрывчатых веществ. При этом заряд взрывчатого вещества может быть в грунте, багаже пассажиров, кейсе, автомобиле и т.д.

К сожалению, эффективность поиска зависит от психофизиологического состояния собаки. Собаки должны постоянно тренироваться. Пропуски в работе или тренировке более 1-2 месяцев недопустимы. При высокой температуре (свыше +25-30°С) собаки способны работать не более 30-40 минут, а затем требуется отдых в тени как минимум в течение 1-2 часов. Желательно, чтобы при поиске взрывчатых веществ собаку не отвлекали посторонние люди, шум техники и т.д.

Обнаружение радиоуправляемых взрывных устройств может осуществляться путем использования метода нелинейной радиолокации. Существующие отечественные переносные приборы нелинейной локации "Октава", "Обь", "Онега", а также зарубежные приборы предназначены для обнаружения устройств, содержащих полупроводниковые элементы (транзисторы, диоды, микросхемы и т.п.) в своей конструкции. Электронная схема объекта поиска (взрывного устройства) может находиться как во включенном, так и в выключенном состоянии. С помощью этих при-

боров возможно также обнаружение взрывных устройств, содержащих электронные таймеры (временные взрыватели).

Объекты поиска могут располагаться в полупроводящей среде (грунте, воде, растительности), а также в стенах зданий, столах, внутри автомобилей и других местах. Поиск затруднен только в непосредственной близости от ЭВМ, факсов, некоторых современных телефонов и других устройств, содержащих полупроводниковые радиодетали в своей конструкции. Приборы нелинейной локации состоят из антенного устройства (на телескопической штанге) и приемо-передающего блока. Для расширения тактических возможностей прибора в приемном и передающем устройствах предусмотрена регулировка как чувствительности, так и мощности. Контроль работоспособности прибора осуществляется с помощью нелинейного имитатора.

Приборы нелинейной локации работают как правило в дециметровом диапазоне радиоволн. Их характерные размеры составляют 0,2-0,4 м, масса - до 4-8 кг. Дальность обнаружения взрывного устройства с радиоэлектронными устройствами - до 1,5-2 м. Время работы от автономных источников питания - до 4-6 часов.

Впрочем, необходимо отметить, что в отдельных случаях возможен подрыв простейших неэкранированных самодельных радиоуправляемых взрывных устройств при поднесении к ним вплотную антенного устройства прибора нелинейной локации. За рубежом выпускаются специальные переносные "уничтожители бомб" (Bomb Ranger), подрывающие радиоуправляемые взрывные устройства путем быстрого перебора возможных команд управления на расстоянии до 1 км. Установленный заранее в охраняемый автомобиль он вызовет подрыв взрывного устройства и спасет жизнь владельца автомобиля.

Взрывные устройства с часовым замыкателем (взрывателем) могут обнаруживаться путем использования портативных контактных микрофонов (фонендоскопов). Эти приборы позволяют снимать акустическую информацию через стены, потолки и другие ограждающие конструкции вокруг взрывного устройства. Для снижения уровня внешних шумов датчик необходимо закреплять на герметике в тех местах ограждающих конструкций, где они тоньше всего и не очень плотны.

Проводные линии управления взрывного устройства можно обнаруживать в полевых условиях путем применения переносных электромагнитных кабелеискателей (R-210, Р-480 - США и т.п.). Они включают в себя передающий и приемный блоки, закрепляемые на концах несущей штанги длиной 1-1,4 м. Рабочие частоты 40-100 кГц. Глубина обнаружения находящихся в грунте кабельных линий управления - до 1 м. Расчет - 1 человек, скорость ведения поиска - до 2-3 км/ч. Масса приборов - до 4-6 кг.

Металлические элементы конструкции взрывного устройства могут обнаруживаться с применением переносных и стационарных ("ворота") металлоискателей. В них используются два метода обнаружения - индукционный или магнитометрический. Первый обеспечивает обнаружение как цветных, так и черных металлов. Второй - только черных (сталь и ее сплавы), но он более чувствителен, чем первый метод.

Например, отечественные индукционные портативные детекторы металлов АКА-7202 (масса 0,4 кг) и "СТЕРХ-92АР" (масса 1,5 кг) обеспечивают обнаружение пистолета на расстоянии до 0,4-0,6 м, автомата - до 1-1,2 м. Более чувствительный прибор "СТЕРХ-92АР" обеспечивает кроме того селекцию предметов на черные и цветные металлы. Дальность обнаружения металлических предметов в грунте и пресной воде практически такая же, как и в воздухе. Отечественный металлоискатель арочного типа ("ворота"), марка ОСТ-751, служит для обнаружения металлических предметов при проходе через дверной проем, арочную перегородку и т.д. Возможна настройка чувствительности непосредственно на конкретный предмет (гранату, пистолет, холодное оружие и др.). Ширина арочного проема 90-120 см. Прибор предназначен для использования в банках, офисах, таможенных службах и других организациях для пресечения несанкционированного проноса оружия, аппаратуры, взрывных устройств, драгоценных металлов.

Весьма удобны и надежны в эксплуатации феррозондовые металлоискатели фирмы ФЕРСТЕР (Германия), использующие магнитометрический метод обнаружения. Из наиболее миниатюрных зарубежных индукционных металлоискателей следует отметить прибор LBD-105 (США), предназначенный для быстро-

го осмотра людей, багажа, офисной мебели и т.п. в целях обнаружения взрывных устройств, стрелкового и холодного оружия.

Неоднородности вмещающей среды в месте установки взрывного устройства можно регистрировать с помощью спектрозональных и поляризационных портативных оптических приборов. Подобные переносные приборы используются в строительстве для дистанционного контроля качества различных конструкций (железобетонных и металлических балок, опор и т.д.).

В ночное время эффективно применение малогабаритной тепловизионной аппаратуры, обладающей разрешающей способностью в десятые доли градуса Цельсия.

Взрывные устройства, установленные в грунте, могут быть обнаружены также с использованием щупов. Наконечники щупов необходимо изготавливать из твердых неметаллических материалов (ситалла и т.п.), что исключит подрыв при использовании противощупных электрических замыкателей.

Характерные признаки формы взрывных устройств и оружия, находящихся в багаже, можно выявлять, используя стационарную рентгеновскую аппаратуру, работающую на "проход". Она используется в санках, офисах и других местах.

Необходимо отметить, что ни один из рассмотренных методов обнаружения не может в полной мере обеспечить надежность обнаружения взрывного устройства. Целесообразно комплексно использовать методы и поисковую аппаратуру. Наибольшая безопасность обеспечивается при этом за счет применения телеуправляемой роботизированной техники.

Средства поиска взрывных устройств постоянно совершенствуются. Так, например, В США проектируется установка, которая способна находить бомбы на расстоянии, тем самым обеспечивая дополнительную безопасность как мирным гражданам, так и армии.

Для поиска взрывных устройств используются самые разные методы — от специальных рентгеновских аппаратов до масс-спектрометров и установок газовой хроматографии. Но в любом случае подозрительный объект должен находиться относительно недалеко от детектирующей системы.

Исследователи из Университета Вандербильта (США) под руководством инженера Дугласа Адамса проектируют установку,

которая будет способна обнаруживать бомбы на расстоянии, обеспечивая дополнительную степень безопасности.

Разработка состоит из фазированного акустического массива, который фокусирует звуковой пучок высокой интенсивности на подозрительном предмете (в опытах используется импровизированное взрывное устройство). Одновременно лазерный виброметр, нацеленный на оболочку потенциальной взрывчатки, регистрирует вибрации, вызванные воздействием акустических волн. Анализ характеристик этих колебаний позволяет установить, что находится внутри объекта.

В экспериментах использовались два муляжа, один из которых содержал компоненты, имитирующие физические свойства взрывчатки небольшой мощности, другой — высокой мощности. Образцы были покрыты акриловой смолой, играющей роль пластикового контейнера. Лазерный виброметр при этом фокусировался на верхней части предполагаемого взрывного устройства.

Тестирование показало чёткие различия в структуре вибраций, вызванных воздействием акустических волн на образцы с разными материалами.

Во время другого опыта команда Дугласа Адамса продемонстрировала, что акустический метод позволяет выявить различия между пустым контейнером, ёмкостью с жидкостью (в испытаниях применялась вода) и пластичным веществом (глиной). Использовались контейнеры от молока объёмом около 3,8 л. В ответ на акустическое воздействие на поверхности пустой тары фиксировались вибрации максимальной амплитуды, а резервуара с глиной - минимальной.

Наконец, было установлено, что для анализа содержимого предметов в твёрдой оболочке, в частности металлической, лучше использовать ультразвуковые волны. При работе с объектами в оболочке из пластика можно применять дозвуковые и инфразвуковые волны.

Данный метод, как и многие другие, разрабатываемые в различных странах мира, в том числе и в России, будут способствовать ускорению поиска и обнаружения взрывных устройств.

Яриков И.В.,
курсант 4 курса
Краснодарского университета МВД России
научный руководитель:
Александров А.Г.,
преподаватель кафедры ИБ
Краснодарского университета МВД России

Средства контроля за передвижением транспорта

К средствам контроля за передвижением транспорта можно отнести аппаратно-программный комплекс (АПК) «Коридор безопасности» - это система диспетчерского управления автомобильным транспортом, перевозящим специальные грузы, предназначенная для автоматизации процесса управления транспортными средствами с целью повышения уровня их безопасности, соблюдения экологических требований в процессе перевозки опасных грузов и повышения экономической эффективности предприятий - грузоперевозчиков.

Основой АПК «Коридор безопасности» являются спутниковые диспетчерские системы, в которых транспортные средства определяют свое местонахождение с помощью глобальных спутниковых систем ГЛОНАСС и /или GPS, а результаты местоопределения по каналам связи передают в диспетчерские центры.

Центральным звеном спутниковой системы диспетчерского управления городским и пригородным автомобильным транспортом, перевозящим специальные грузы, является диспетчерский центр предприятия-грузоперевозчика, обеспечивающего указанные перевозки. В МВД России безопасность транспорта, перевозящим специальные грузы, обеспечивает межрегиональный координационный центр (МКЦ) ГУВО МВД России.

Объектами управления являются закрепленные за ним автомобили, перевозящие специальные грузы. Взаимодействующими с диспетчерским центром организациями являются территориальные органы исполнительной власти (Ространснадзор, МВД (ГИБДД) и МЧС России) и предприятия - грузоотправители (грузополучатели).

Основными функциями системы диспетчерского управления транспортными средствами, перевозящими специальные грузы, являются следующие:

1.Мониторинг, заключающийся в:

- контроле местонахождения транспортных средств, маршрута следования, скоростного режима;

- контроле состояния транспортных средств, их водителей, состояния грузов и условий перевозки.

2. Принятие управленческих решений на основе мониторинговой и другой актуальной информации.

3. Доведение до исполнителей (водителей, сопровождающих груз лиц, работников транспортной компании, взаимодействующих организаций) принятых управленческих решений.

4. Контроль исполнения принятых решений.

Система информационного сопровождения и мониторинга городских и пригородных автомобильных перевозок опасных грузов не может подменять действующие системы диспетчерского управления. Она должна обеспечивать их актуальными и достоверными данными, т.е. являться информационной, но не управляющей системой. Поэтому на рассматриваемую систему следует возлагать только функции мониторинга, сбора, обработки, представления и отображения полученных данных, а также, возможно, функции информационного обмена, в том числе с взаимодействующими организациями. При этом формирование и согласование с ГИБДД схем движения транспортных средств, оперативное управление (формирование команд водителю, принятие решений о задействовании резервных транспортных средств и т.п.) не должно возлагаться на эту систему. Однако вся информация, необходимая для контроля перевозок органами внутренних дел и организации реагирования на внештатные ситуации, должна передаваться в дежурные части органов внутренних дел. В распространенных ныне системах мониторинга этот вопрос, как правило, не решен. В лучшем случае, органы внутренних дел информируются о уже имевшем место происшествии по каналам телефонной связи, без достаточной конкретизации сведений о характере происшествия и текущем местонахождении транспортного средства.

Для определения местоположения транспортного средства могут использоваться навигационные системы. Навигация это определение координатно-временных параметров объектов.

Системы навигации и позиционирования предназначены для постоянного контроля за местонахождением (состоянием) объектов. В настоящее время существует два класса средств навигации и позиционирования: наземные и космические.

К наземным относят стационарные, возимые и переносные системы, комплексы, станции наземной разведки, иные средства навигации и позиционирования. Принцип их действия заключается в контроле радиоэфира посредством специальных антенн, подключаемых к сканирующим радиостанциям, и выделении радиосигналов, излучаемых радиопередатчиками объектов слежения или излучаемых самим комплексом (станцией) и отраженных от объекта слежения либо от специальной метки или кодового бортового датчика (КБД), размещенных на объекте. При использовании такого рода технических средств имеется возможность получить информацию о координатах местонахождения, направлении и скорости перемещения контролируемого объекта. При наличии на объектах слежения специальной метки или КБД устройства идентификации, подключаемые к системам, позволяют не только отмечать местоположение контролируемых объектов на электронной карте, но и соответствующим образом различать их.

Космические системы навигации и позиционирования разделяются на два типа.

Первый тип космических систем навигации и позиционирования отличает применение на мобильных объектах слежения специальных датчиков – приемников спутниковой навигационной системы типа ГЛОНАСС (Россия) или GPS (США). Навигационные приемники подвижных объектов слежения принимают от навигационной системы радиосигнал, который содержит координаты (эфемериды) спутников на орбите и отсчет времени. Процессор навигационного приемника, по данным от спутников (как минимум, от трех) рассчитывает географические широту и долготу его местонахождения (приемника). Эта информация (географические координаты) может быть визуализирована как на самом навигационном приемнике, при наличии устройства вывода информации (дисплея, монитора), так и в пункте слеже-

ния, при ее передаче от навигационного приемника подвижного объекта посредством радиосвязи (радиальной, конвенциональной, транкинговой, сотовой, спутниковой).

Второй тип космических систем навигации и позиционирования отличает сканирующий прием (пеленг) на орбите сигналов, поступающих от радиомаяков, установленных на объекте слежения. Спутник, принимающий сигналы от радиомаяков, как правило, сначала накапливает, а затем в определенной точке орбиты передает информацию об объектах слежения в наземный центр обработки данных. Время доставки информации при этом несколько увеличивается.

Спутниковые навигационные системы позволяют:

осуществлять непрерывный контроль и слежение за любыми подвижными объектами;

отображать на электронной карте диспетчера координаты, маршрут и скорость движения объектов контроля и слежения (с точностью определения координат и высоты над уровнем моря до 100 м, а в дифференциальном режиме – до 2…5 м);

оперативно реагировать на внештатные ситуации (изменение ожидаемых параметров на объекте контроля и слежения либо в его маршруте и графике движения, сигнал SOS и т. д.);

оптимизировать маршруты и графики движения объектов контроля и слежения.

В настоящее время функции специализированных систем навигации и позиционирования (автоматическое отслеживание текущего месторасположения абонентских аппаратов, терминалов связи с целью обеспечения роуминга и предоставления услуг связи) с относительной точностью могут выполнять спутниковые и сотовые (при наличии на базовых станциях аппаратуры определения местонахождения) системы радиосвязи.

Широкое внедрение систем навигации и позиционирования, повсеместная установка соответствующей аппаратуры в сетях сотовой связи России с целью определения и постоянного контроля местонахождения работающих передатчиков, патрулей, транспорта, иных объектов, представляющих интерес для органов внутренних дел, могло бы значительно расширить возможности правоохранительной деятельности.

Основной принцип определения местоположения с помощью спутниковых навигационных систем – использование спутников в качестве точек отсчета.

Для того, чтобы определить широту и долготу наземного приемника, приемник должен получать сигналы не менее чем от трех спутников и знать их координаты и расстояние от спутников до приемника. Координаты измеряются относительно цента земли, который имеет координату (0, 0, 0).

Расстояние от спутника до приемника вычисляется по измеренному времени распространения сигнала. Эти вычисления выполнить несложно, так как известно, что электромагнитные волны распространяются со скоростью света. Если известны координаты трех спутников и расстояния от них до приемника, то приемник может вычислить одно из двух возможных мест в пространстве. Обычно приемник может определить, какая из этих двух точек действительная, так как одно значение местоположения имеет бессмысленное значение. На практике, для исключения ошибки часов генератора, которое влияет на точность измерений разницы во времени, необходимо знать местоположение и расстояние до четвертого спутника.

В настоящее время существуют и активно используются две спутниковые навигационные системы – ГЛОНАСС и GPS.

Спутниковые навигационные системы включают в себя три составные части.

космический сегмент, в который входит орбитальная группировка искусственных спутников Земли (иными словами, навигационных космических аппаратов);

сегмент управления, наземный комплекс управления (НКУ) орбитальной группировкой космических аппаратов;

аппаратура пользователей системы.

Космический сегмент системы ГЛОНАСС состоит из 24 навигационных космических аппаратов (НКА), находящихся на круговых орбитах высотой 19100 км, наклонением 64,5° и периодом обращения 11 ч 15 мин в трех орбитальных плоскостях. В каждой орбитальной плоскости размещаются по 8 спутников с равномерным сдвигом по широте 45°.

Космический сегмент навигационной системы GPS состоит из 24 основных НКА и 3 резервных. НКА находятся на шести

круговых орбитах высотой около 20000 км, наклонением 55°, равномерно разнесенных по долготе через 60°.

Наземный сегмент обеспечивает эфемеридное обеспечение спутников. Это означает, что на земле определяются параметры движения спутников и прогнозируются значения этих параметров на заранее определённый промежуток времени. Параметры и их прогноз закладываются в навигационное сообщение, передаваемое спутником наряду с передачей навигационного сигнала. Сюда же входят частотно-временные поправки бортовой шкалы времени спутника относительно системного времени. Измерение и прогноз параметров движения НКА производятся в Баллистическом центре системы по результатам траекторных измерений дальности до спутника и его радиальной скорости.

Аппаратура пользователей системы это радиотехнические устройства, предназначенные для приема и обработки радионавигационных сигналов навигационных космических аппаратов для определения пространственных координат, составляющих вектора скорости движения и поправки шкал времени потребителя глобальной навигационной спутниковой системы.

Для обеспечения высокой надежности и достоверности передачи мониторинговой информации от бортового оборудования автотранспорта подразделений МВД России в дежурные чисти в составе системы необходимо использовать резервный канал передачи данных, в качестве которого можно использовать УКВ-радиосвязь.

СОДЕРЖАНИЕ

Научное издание

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ, ТЕРРОРИЗМУ И ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ

Материалы
межвузовской научно-практической конференции,
посвященной Дню российской науки

10 февраля 2014 г.

В авторской редакции
Компьютерная верстка *Н. А. Никитина*

978-5-9266-0853-0

9 785926 608530

Подписано в печать 05.02.2015. Формат 60x84 1/16.
Усл. печ. л. 12,1. Тираж 500 экз. Заказ 198.

Краснодарский университет МВД России.
350005, Краснодар, ул. Ярославская, 128.