ИБРАЕВ Ч.К.
lib.knu@mail.ru

ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ ИНФОРМИРОВАНИЯ И ТАКТИКИ ЗАЩИТЫ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ ПО ВЫЯВЛЕНИЮ И РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ

Вопросы криминалистической тактики – одни из наиболее разработанных в криминалистике.

Известно, что в своем изначальном смысле тактика представляет собой теорию и практику подготовки и ведения боя и понятие «криминалистическая тактика», естественно, несет элемент условности, так как нельзя говорить о военных действиях, ведущихся государством против своих граждан, даже если они не законопослушны.

Криминалистическая тактика традиционно представлена в криминалистике одним из разделов, и Р.С. Белкин определял ее следующим образом: «Криминалистическая тактика – это система научных положений и разрабатываемых на их основе рекомендаций по организации и планированию предварительного и судебного следствия, определению линии поведения лиц, осуществляющих доказывание, и приемов проведения отдельных следственных и судебных действий, направленных на собирание и исследование доказательств, на установление причин и условий, способствовавших совершению и сокрытию преступлений»[1].

А.В. Дулов, Г.И. Грамович, А.В. Лапин определяли тактику как выбор способа действия. «Тактика – это выбор оптимального способа действия в условиях противоборства, несовпадения интересов, участвующих в определенной деятельности лица»[2].

Криминалистическая тактика рассматривается в основном как тактика различных следственных действий. Наиболее актуальна роль тактических приемов и комбинаций при ведении расследования в условиях противодействия, что наиболее ярко отразилось в дефиниции, даваемой О.Я. Баевым: «Под тактикой следственных действий мы понимаем систему научных положений и разрабатываемых на их основе соответствующих средств (тактических рекомендаций, тактических приемов, тактических операций) допустимого и рационального собирания, использования и исследования доказательственной информации следователем при производстве отдельных следственных действий в условиях потенциального или реального, непосредственного или опосредованного противодействия со стороны лиц, преимущественно не заинтересованных в установлении истины при расследовании преступлений»[3].

Известно, что использование тактических приемов, комбинаций и операций связано с рядом условий и принципов: правомерностью, допустимостью, научной обоснованностью, целесообразностью их применения и доступностью.

Вопросы организации следствия традиционно включались в раздел криминалистической тактики. Однако в последнее время можно встретить учебники криминалистики с пятичастным делением, в которых вопросы организации следствия выделены в отдельный раздел, что связано с рядом явлений и процессов, существующих в современном следствии: широком использовании бригадного метода расследования, наличия проблем, не решаемых в пределах криминалистической тактики.

Организация и тактика защиты информации в ДВРП имеет ряд особенностей, связанных с тем, что процесс выявления и раскрытия преступлений есть процесс

---

[1] Белкин Р.С., Лившиц Е.М. Тактика следственных действий. - М: Новый Юристъ, 1997. - С. 3.
[2] Криминалистика: Учеб. пособие/А.В. Дулов, Г.И. Грамович, А.В. Лапин и др./ Под ред. А.В. Дулова. - Мн.: Экоперспектива, 1996. - С. 261.
[3] Баев О.Я. Тактика следственных действий. - Воронеж: МОДЕК, 1995. – С.4.

ретроспективного познания – познания события имевшего место в минувшем прошлом – реинциндентики[4], в то время как защита информации – процесс, направленный на события будущего, или, в крайнем случае, настоящего. Действительно, защита информации предполагает мероприятия по предупреждению, выявлению и блокированию возможных, потенциальных информационных угроз до их появления, а также в случае неэффективности указанных действий – планирование и реализацию борьбы с реально существующими угрозами путем минимизации потерь.

Следовательно, организацию информирования и тактику защиты информации в деятельности по выявлению и раскрытию информации мы можем определить как систему научных положений и разработанных на их основе организационных и тактических средств, направленных на обеспечение информационной безопасности системы ДВРП в условиях потенциального или реального, непосредственного или опосредованного противодействия со стороны субъектов преступной деятельности.

Организационный и тактический потенциал мероприятий по защите информации, проводимых в ходе расследования преступления, использования средств и методов обеспечения информационной безопасности включает в себя информацию, представленную в реальной и потенциальной форме, которая может быть получена субъектом ДВРП и использована в целях оптимизации информационных процессов и потоков в деятельности органов дознания и следствия.

Защита информации как процесс, совокупность проводимых мероприятий имеет несколько направлений. В.А. Герасименко, А.А. Малюк выделяют техническую, программную, организационно-правовую и криптографическую защиту[5]. Шиверский А.А. различает три уровня защиты информации в обществе и государстве:

- социально-политический, включающий в себя проведение единой государственной информационной политики;
- организационно-правовой (стратегический), представленный системой нормативно-правовых актов, стандартов, ведомственных инструкций, приказов и т.д.;
- тактический, обеспечивающий реализацию концепции и стратегии защиты информации на конкретном предприятии, учреждении, организации. В целях защиты информации в деятельности по выявлению и раскрытию преступлений выделим два уровня проводимых мероприятий:

1) организационный, охватывающий вопросы организации, планирования и осуществления мер по защите информации в системе ДВРП, в целом и включающий вопросы создания нормативной базы защиты информации в системе ДВРП – ведомственных инструкций и приказов, направленных на обеспечение информационной безопасности, а также обеспечения защиты территорий, помещений, транспортных средств, информационно-вычислительных центров и вычислительных сетей, архивов системы и хранимых в них информационных ресурсов, обеспечение физической и психологической безопасности сотрудников органов дознания и следствия и др. вопросы;
2) тактический, направленный на мероприятия по защите информации в пределах следствия по конкретному уголовному делу.

Грань между данными уровнями весьма условна, т.к. первый и второй уровень взаимодополняющие, однако наличие их предопределено двухуровневой структурой управления деятельностью.

Рассматривая направления защиты информации, следует отметить, что выделение отдельно правовой защиты информации в системе ДВРП не совсем обоснованно, так как мероприятия всех остальных направлений должны лежать в правовой сфере.

---

[4] Каминский М.К. Что есть, что может быть и чего быть не может для системы криминалистика» // Криминалистика, криминология и судебные экспертизы в свете системно-деятельностного подхода. Вып.3. -Ижевск: Детектив-информ, 2001. - С. 7-9.

[5] Герасименко В.А., Малюк А.А. Основы защиты информации. - М., 1997. - С. 284-285.

Правовая защита информации предполагает регламентацию деятельности службы собственной безопасности системы ДВРП; наличие в должностных инструкциях обязательств по защите информации, сведений, составляющих тайну, к которой допущен сотрудник в связи с занимаемой должностью и выполняемой работой; регламентацию системы разграничения доступа персонала к сведениям, составляющим тайну следствия и служебную тайну органов следствия и дознания; страхование сотрудников, их близких и имущества от рисков, связанных с родом выполняемых обязанностей; регламентацию правил обращения персонала с информацией; регламентацию защищенного документооборота и архивного хранения документов и их массивов; страхование ценных бумажных и электронных документов и их массивов от различных рисков (пожаров, стихийных бедствий и иных); регламентацию использования технических средств защиты информации; создание и регламентацию деятельности аналитической службы системы ДВРП и др. меры.

Криптографическая защита информации может быть реализована либо аппаратными средствами, либо программными, поэтому в практическом плане ее следует отнести к техническим средствам защиты.

В связи с вышесказанным мы выделяем нижеуказанные направления защиты информации в деятельности по выявлению и раскрытию преступлений.

Техническая защита информации, включает защиту информации аппаратными, программными средствами, а также применение криптографических методов защиты. К аппаратным средствам защиты информации относятся: средства защиты технических каналов утечки информации, возникающие при работе электронно-вычислительных машин, средств связи, офисного оборудования (копировальных и факсимильных аппаратов и т.д.); технические средства защиты помещений от технических средств разведки; технические средства разграничения доступа; шифровальная техника, средства противопожарной охраны территорий и помещений. К программным средствам защиты относятся: математические и программные средства разграничения доступа к ресурсам электронно-вычислительных машин и компьютерных сетей, программные средства идентификации и верификации пользователей, использование специальных программных средств защиты, программы и их комплексы, реализующие криптографические методы закрытия информации, защищенные электронные документы и базы данных, а также правила работы пользователей на электронно-вычислительных машинах и компьютерных сетях.

Организационно-управленческая защита информации, включает в себя совершенствование кадрового обеспечения (отбор, обучение и инструктаж сотрудников), осуществление пропускного режима на территорию, в здания и помещения, идентификацию сотрудников, охрану и обеспечение безопасности сотрудников и их близких родственников, родственников и близких лиц, упорядочение взаимодействия со средствами массовой информации, ведение и использование защищенного документооборота, ведение аналитической работы по выявлению информационных угроз, потенциальных и реальных каналов утечки информации, осуществление организационных вопросов использования технических средств защиты информации и т.д.

Тактическая защита информации – приемы, комбинации и операции, осуществляемые по обеспечению информационной безопасности расследования события преступления, выявления и блокирования утечек информации в следствии.

Организационные средства защиты при этом играют особую роль, так как позволяют непосредственно, или в комплексе с другими средствами решать возникающие проблемы, в то время как другие средства без организационных мероприятий малоэффективны. Организационные средства позволяют объединить другие средства в единую систему защиты.

Мероприятия по защите информации, проводимые в ходе расследования события преступления, могут быть разделены на несколько этапов.

Первый этап посвящен решению вопроса о вероятности утечки информации при расследовании конкретного события преступления. Характер конкретного уголовного дела, расследуемого события преступления и следственных ситуаций, возникающих в ходе расследования, во многом предопределяют рассмотрение и решение проблем оценки, хранения и использования информации в процессе следствия. Ответы на вопросы: насколько возможно противодействие и организация преднамеренной утечки информации при расследовании данного дела влияют на принятие решения о необходимости построения системы защиты информации в пределах конкретного следствия и характеристиках расследуемой системы.

Возможность утечки информации должна рассматриваться исходя не только из характера конкретного уголовного дела, но и существующей следственной ситуации. «Следственная ситуация – совокупность условий, обстановка, в которой в данный момент протекает процесс доказывания»[6]. Сочетание совокупности компонентов следственной ситуации (информационного, психологического, процессуального и тактического, материального и организационно-тактического характера) предопределяет наличие необходимости применения в ходе расследования средств и методов защиты информации, а также конкретный набор проводимых мероприятий и используемых тактических приемов и комбинаций.

При положительном решении вопроса о возможности утечки информации встает вопрос о потенциальном объекте разведки субъектов преступной деятельности, таковым может быть с большей или меньшей вероятностью любой источник информации и (или) ее носитель. Поэтому следующим этапом является выявление реального состава информации и ее носителей, требующих защиты.

Для определения возможности утечки информации с того или иного источника (носителя) необходимо ранжирование информации. При ранжировании должны быть учтены следующие характеристики информации и ее носителя: ценность информации, вид охраняемой законом тайны, степень секретности или конфиденциальности информации, доступность и защищенность источника или носителя, количество лиц, фактически допущенных к информации и ее носителю, а также социально-психологические черты данных лиц.

По мнению специалистов по защите информации, степень защищенности информации может определяться одним из следующих основных способов.

По соответствию защищенности действующим стандартам. Для построения системы защиты информации в процессе расследования конкретного события преступления данный метод не применим, так как невозможна выработка стандарта с учетом особенностей всякого расследования и возникающих следственных ситуаций.

Соотношением стоимости информации и стоимости организации и осуществления защиты. Подобный подход не всегда применим, так как во многих случаях невозможно определить стоимость информации. Данный вариант определения степени защищенности оправдан в случае закрытия сведений, составляющих коммерческую тайну, но абсолютно не применим к личной тайне, персональным данным граждан и, конечно, тайне следствия и служебной тайне органов следствия и дознания.

Соотношением времени, потраченного на построение системы защиты и времени преодоления данной системы.

[6] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Российская Е.Р. Криминалистика: Учебник для вузов/Под ред. проф. Р.С. Белкина. - М.: НОРМА, 2001. - С. 46.