Концепция информационной безопасности правоохранительной сферы в парадигме открытых систем

Овчинский Анатолий Семенович,
начальник учебно-научного комплекса информационных технологий Московского университета МВД России,
д.т.н., профессор, полковник полиции

Угрозы безопасности. Информационные технологии правоохранительной деятельности открыли фантастические возможности в моделировании и прогнозировании событий, в отслеживании и контроле ситуаций, в управлении технологическими и социальными процессами. Одновременно современные технологии принесли и новые угрозы.

Традиционные представления о безопасности как состоянии защищенности жизненно важных интересов требуют переосмысления на новых научных основах. Совершенствуя только технологии защиты, сейчас невозможно обеспечить безопасность ни самой информации, ни ее обладателей, как невозможно победить в войне, рассчитывая только на оборону. Обеспечение информационной безопасности в деятельности правоохранительных органов должно включать использование как защитных, так и наступательных средств, а также совершенствование инструментов получения собственно информации.

Триединство информации. Методологическую основу информационной безопасности в деятельности правоохранительных органов составляют представления о триединстве информации в открытых системах социальных связей и психологических отношений.

Во-первых, информация возникает в процессе реакций на воздействия, которые испытывают объекты природы на разных уровнях жизни. Эта реактивная информация рождается в сознании человека в процессе целевой интерпретации того, что он видит, слышит, ощущает, осязает, чувствует. Получение именно реактивной информации является целью многих видов деятельности. Она позволяет понимать смысл происходящего, принимать решения, совершать поступки, действовать адекватно ситуации.

Во-вторых, информация накапливается на определенных носителях. Эволюция живой природы связана с накоплением и передачей биологической ресурсной информации. В генетических кодах, в строении органов и тканей, в обменных процессах мы видим проявление ресурсной информации. Все существенные этапы развития цивилизации связаны с более совершенными технологиями накопления и передачи социальной ресурсной информации.

В-третьих, информация в качестве фона отражает окружающую нас реальность, как в доступных, так и в недоступных для восприятия формах. Эта фоновая информация подобно 25-му кадру может обходить защитные функции сознания. Фоновые воздействия могут вызывать заданные психические реакции и запрограммированные действия и поступки.

Оперирование понятиями реактивность, ресурность и фоновость открывает новые ракурсы в понимании самых разнообразных явлений, поскольку вся жизнь построена на информационных взаимодействиях.

Компоненты инфобезопасности. Обратившись к проблемам информационной безопасности, мы должны отдать приоритет реактивной информации, позволяющей принимать решения, адекватные ситуации и понимать суть происходящего. Это означает, что технологии добывания, обработки и анализа данных являются необходимым компонентом обеспечения инфобезопасности. Именно наличие реактивной информации позволяет правоохранительным органам выполнять свои функции эффективно и в полном объеме.

Не менее важны технологии инженерно-технической, аппаратно-программной, криптографической и стеганографической защиты информации. При этом наряду с обеспечением безопасности защищаемой реактивной информации основное внимание необходимо уделять защите информационных ресурсов.

Третье направление информационной безопасности в настоящее время приобретает особую остроту, поскольку самым уязвимым звеном безопасности остается человек. Так, необходимым компонентом обеспечения безопасности является противодействие негативным и деструктивным информационно-психологическим воздействиям, инструментом которых может быть фоновая информация.

Получение информации. Не отрицая неразрывную связь информационного и аналитического обеспечения правоохранительной деятельности, необходимо концептуально представлять разницу между ними.

Информационное обеспечение — это, в первую очередь, деятельность по созданию, поддержанию и совершенствованию ресурсов оперативно-розыскных, криминалистических и криминологических данных, сведений

и знаний. Это формирование единого пространства ресурсов структурированных данных и сведений, доступных для оперативного использования.

В свою очередь, аналитическое обеспечение заключается в получении уже реактивной информации, позволяющей принимать решения и осуществлять действия, нацеленные на конкретный результат по профилактике, предотвращению, пресечению преступной деятельности, раскрытию и расследованию преступлений, охране общественного порядка. Это требует применения методов идентификации, диагностики, прогнозирования с использованием автоматизированных комплексов логико-аналитической обработки и визуализации данных.

Неисчерпаемым источником информационных ресурсов и генератором реактивной информации является фоновая информация — многомиллионные массивы сообщений, результаты видеонаблюдений, акустического контроля, мониторинга радиоэфира, телекоммуникаций, средств массовой информации, Интернета. На свойствах фоновой информации строятся стратегические операции и тактические приемы непроцессуального использования оперативно-розыскной информации, информационно-психологических воздействий, информационного противоборства в борьбе с наиболее опасными криминальными явлениями.

Защита информации. Обращая внимание на необходимость комплексного подхода к обеспечению безопасности собственно информации, необходимо выделять технологии защиты реактивной информации, получение которой является целью оперативно-розыскного и следственного процесса и технологии защиты ресурсной информации, накапливаемой на определенных носителях.

В комплексе инженерно-технических мер защиты реактивной информации необходимо выделить поиск и нейтрализацию работы действующих каналов утечки информации (оптических, акустических, электрических, электромагнитных), препятствие возможности создания оперативно-технических позиций для скрытого перехвата сигналов, энергетическое сокрытие сигналов, препятствующее их распознанию, регистрации и восстановлению противником.

При защите информационных ресурсов наряду с инженерно-техническими мерами, направленными на предотвращение доступа противника к носителям информации и средствам информации, аппаратно-программной и криптографической защитой от злоумышленных разрушений, искажений и хищений информации необходимо обратить внимание на угрозы, связанные с качеством данных.

Нельзя не учитывать неаддитивность вклада отдельных факторов в состояние открытых систем. Так, наличие предателя или законспирированного врага — «крота» сводит на нет все усилия по защите информации. Технологии защиты информации при этом должны включать информационно-психологическое противоборство, контроль, воздействия, связанные с фоновой информацией.

Информационные воздействия. Касаясь технологий информационного противоборства, необходимо представлять, что управление людьми, сообществами, народами все в большей мере осуществляется с помощью целенаправленных информационных воздействий.

Технологии информационно-психологического противоборства должны опираться на представления о функциональных (обеспечивающих) проявлениях информации как источника и генератора социально-психологической энергии. Именно информация в открытых системах социальных связей и психологических отношений создает потенциалы социально-психологической энергии, которая необходима для решений, поступков и действий в различных ситуациях.

С другой стороны, любое проявление социальной активности связано с разрядкой энергии, и именно информационные воздействия вызывают психологические, интеллектуальные и эмоциональные реакции, порождающие уже события и их последствия.

Развитие представлений о непрерывной череде энергоинформационных трансформаций требует вскрытия угроз, связанных с энергоинформационной безопасностью человека как объекта живой природы и субъекта социальных отношений, обладающего внутренним духовным миром и свободой воли.

Триединство инфобезопасности. Технологии обеспечения информационной безопасности в открытых системах социальных связей и психологических отношений должны стать действенным инструментом правоохранительной деятельности, построенной на новых организационных основах. Они должны включать как защитные, так и наступательные меры информационного противоборства, применение всего комплекса современных средств и методов добывания, обработки, анализа и использования информации в триединстве ее реактивных, ресурсных и фоновых проявлений.

Данная Концепция заложена в основу подготовки сотрудников полиции по новой специальности — «Безопасность информационных технологий», утвержденной решением Правительства Российской Федерации.