Рассматривая второй вопрос, можно отметить, что инструментарий может быть применен различный, но важно учитывать, с одной стороны, ограниченный характер методов для различных прикладных задач, с другой – важно не перейти порог избыточности, чтобы не получилась модель ради модели, без ее аналитического компонента.

Как один из вариантов решения вопроса аналитического обеспечения правоохранительной деятельности является использование положений теории графов. И, соответственно, инструментом для проведения анализа информации является разработка в общем виде графовой модели $G = (V, E)$, определения вершин графа $(V1, V2, ..., Vn)$ – управляющих параметров, «параметров порядка», и его дуг $(E1, E2, ... Em)$ для ориентированных графов в части формирования весовых коэффициентов воздействия на управляющие параметры.

Представленный подход является одним из возможных вариантов решения вопроса совершенствования информационно-аналитической деятельности правоохранительных органов в целом и органов внутренних дел в частности. Соответственно, использование математических методов и моделей в этой деятельности, и в первую очередь при анализе информации, позволит существенно повысить достоверность аналитической и прогнозной деятельности в правоохранительной сфере.

УДК 378:147

А.В. Луговая, А.В. Душкин, С.С. Кочедыков

АКТУАЛЬНЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ В ВОРОНЕЖСКОМ ИНСТИТУТЕ ФСИН РОССИИ

Важным этапом совершенствования профессиональной подготовки сотрудников уголовно-исполнительной системы (УИС) является непрерывное повышение образовательного уровня в условиях возрастающей роли информационно-телекоммуникационных технологий (ИТТ).

Внедрение современных ИТТ в деятельность УИС предполагает реализацию комплекса мероприятий, направленных на совершенствование инфраструктуры информационно-телекомуникационных систем (ИТКС), повышение функционирования и развития ведомственной системы передачи и обработки данных, эксплуатируемых автоматизированных информационных систем специального назначения (АИС СН), а также систем информационной безопасности (ИБ) и защиты информации (ЗИ).

С целью успешной реализации указанных направлений необходимо проведение комплекса организационно-правовых, организационно-технических, технологических и кадровых мероприятий, направленных на обеспечение ИБ и ЗИ эксплуатируемых и вновь создаваемых ИТКС и объектов УИС.

В настоящее время в УИС существует потребность в высококвалифицированных кадрах, обладающих специальными компетенциями в области ИБ и технической ЗИ при организации деятельности подразделений ФСИН России. Сотрудники УИС в своей профессиональной деятельности должны:

неукоснительно соблюдать режим секретности;

реализовывать комплекс мер по обеспечению безопасности информации, защиты государственной тайны и персональных данных;

обеспечивать соблюдение специальных требований безопасности информации в сфере защиты государственной и служебной тайны при организации ведомственного документооборота;

обеспечивать защиту персональных данных, обрабатываемых как на бумажных, так и на электронных носителях, в том числе с использованием системы электронного документооборота;

проводить мероприятия по контролю за обеспечением ЗИ, в том числе защиты государственной тайны;

осуществлять информационно-аналитическое обеспечение оперативно-розыскных мероприятий;

применять при выполнении профессиональных задач криминалистическую и специальную технику;

соблюдать и контролировать в профессиональной деятельности требования нормативно-правовых актов при обеспечении режима секретности и защиты государственной тайны с использованием современных технических средств и методов обеспечения ИБ и ЗИ;

применять методы аналитической разведки, осуществлять оперативно-аналитический поиск, оперативно-розыскной анализ информации в ИТКС, а также АИС СН.

Решение обозначенной проблемы влечет за собой необходимость кадрового обеспечения структурных подразделений УИС специалистами инженерно-технического профиля.

Одной из приоритетных задач, обозначенной Программой развития системы ведомственного профессионального образования на период до 2020 года, является оптимизация структуры набора в учебные заведения с учетом кадровых потребностей служб и подразделений УИС.

Воронежский институт ФСИН России является единственной ведомственной образовательной организацией, осуществляющей подго-

товку инженерно-технических кадров для УИС по образовательным программам высшего и дополнительного профессионального образования, а также по программам подготовки научно-педагогических кадров в адъюнктуре.

В целях обеспечения кадрами, обладающими профессиональной компетентностью в области информационной безопасности при организации деятельности подразделений ФСИН России, в 2015 г. в Воронежском институте ФСИН России началась подготовка курсантов по образовательной программе высшего образования 10.05.02 «Информационная безопасность телекоммуникационных систем».

Профессиональная компетентность выпускников в области информационной безопасности образуется из системной интеграции в научно-исследовательской, проектной, контрольно-аналитической, организационно-управленческой и эксплуатационной деятельностях.

В результате освоения образовательной программы у выпускника должны быть сформированы общекультурные, общепрофессиональные, профессиональные и профессионально-специализированные компетенции.

Перечень необходимых для формирования общекультурных, общепрофессиональных и профессиональных компетенций применительно к каждому виду деятельности определяется федеральными государственными стандартами высшего образования. Профессионально-специализированные компетенции соответствуют специализации образовательной программы: в Воронежском институте ФСИН России – сети специальной связи. Среди профессиональных специализированных компетенций выделяются:

способность обеспечить защиту информации в информационных системах учреждений и органов УИС;

способность проводить в учреждениях и органах УИС монтаж и эксплуатацию технических средств защиты информации;

способность осуществлять техническую эксплуатацию в учреждениях и органах УИС современных инфокоммуникационных систем для организации и обеспечения связи, ее развития и совершенствования;

способность организовывать в учреждениях и органах УИС техническую эксплуатацию инженерно-технических средств охраны и надзора (ИТСОН), системы электронного мониторинга подконтрольных лиц и спецтранспорта.

Формирование профессиональной компетентности выпускников осуществляется в ходе изучения дисциплин как базовой части, в том числе дисциплин специализации, определяемые институтом самостоятельно, так и вариативной.

Профессионально-специализированные компетенции формируются в ходе изучения таких дисциплин, как «Информационная безопасность», «Организационно-правовое обеспечение информационной безопасности», «Технические средства и методы защиты информации», «Программно-аппаратные средства и методы защиты информации».

Большую роль играет практическая подготовка курсантов в рамках учебной, производственной и преддипломной практики, проходящей на базе структурных подразделений ФСИН России, особое место среди которых занимает Научно-исследовательский институт информационных технологий ФСИН России, на базе которого курсанты в период прохождения практики формируют профессиональные умения и навыки будущей профессиональной деятельности.

Образовательный процесс в институте обеспечивают высококвалифицированные специалисты, обладающие высоким уровнем научного потенциала, достаточным опытом педагогической работы и практической деятельности. 82 % профессорско-преподавательского состава кафедр имеют ученую степень и звание, 19 % из них – доктора наук, профессора.

Развитая учебно-материальная база института представлена лабораториями и специализированными кабинетами, такими как лаборатория технических каналов утечки информации, лаборатория технической защиты информации, аудитория специальной техники и оперативно-технических мероприятий, на базе которых проводятся учебные занятия по дисциплинам специализации, что позволяет отрабатывать у обучающихся практические профессиональные умения и навыки по избранной специальности в сфере ИБ и ЗИ.

Выпускники Воронежского института ФСИН России по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем» и направлению подготовки 10.07.01 «Информационная безопасность» могут работать в подразделениях инженерно-технического обеспечения и связи учреждений и управлений ФСИН России, в уголовно-исполнительных инспекциях на должностях, связанных с организацией и эксплуатацией сетевого и коммутационного оборудования, инженерно-технических средств обеспечения надзора, информационной безопасности в системах связи и сетях передачи данных, систем электронного мониторинга, а также в научно-исследовательских подразделениях и учебных заведениях УИС.

Исходя из изложенного планируется дальнейшее совершенствование подготовки кадров по информационной безопасности для уголовно-исполнительной системы в Воронежском институте ФСИН России за счет выполнения необходимых мероприятий:

по разработке проекта концепции развития ИБ и ЗИ УИС до 2030 г.;

планированию кадровой обеспеченности подразделений ФСИН России, в которых требуются специалисты в области ИБ и ЗИ;

открытию в Воронежском институте ФСИН России новой специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере», позволяющей готовить универсальных специалистов как юридического, так и технического профиля.

УДК 343

Н.В. Лукашов

СОВРЕМЕННЫЕ МЕТОДЫ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ И ПОДГОТОВКИ КАДРОВ ДЛЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, КОМПЬЮТЕРНЫХ И ИНЫХ ВЫСОКИХ ТЕХНОЛОГИЙ

Термин «высокие технологии» (ВТ) все чаще используется в юридической теории и практике. Однако при этом наблюдается тенденция усугубляющейся неоднозначности трактовки термина, особенно в связи с расследованием преступлений, когда ВТ понимается в узком смысле – синонимом компьютерным информационным технологиям. Так, инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола в разделе «Информационное обеспечение борьбы с преступлениями в области высоких технологий» предусмотрено, что взаимодействующие органы направляют запросы о преступлениях в области высоких технологий, связанных с «неправомерным доступом к компьютерной информации; созданием, использованием и распространением вредоносных программ для ЭВМ; нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети». Данная инструкция фактически ограничивает сферу ВТ сферой информационных технологий (ИТ).

Между тем вне сферы правоохранительной деятельности ВТ трактуются существенно шире и определяется, например, в Большой российской энциклопедии как «совокупность информации, знаний, опыта, материальных средств, используемых при разработке, создании и производстве как новых (ранее неизвестных) продукций и процессов, так и для улучшения качества и удешевления производства известных продуктов».

Исходя из этого понятно, что к ВТ относятся ядерные, космические, генетические, нано- и ряд других технологий, что и подтверждается практикой. Очевидно расхождение между юридической и общепринятой терминологией в определении одной предметной области, а именно сужение общего, родового понятия ВТ до видового ИТ. Это негативно ска-

зывается на эффективности раскрытия и расследования преступлений в данной сфере, имеющих ряд специфических особенностей.

Одной из них является расширенная практика привлечения специалистов и экспертов. Другая особенность – повышенная общественная опасность преступлений в сфере ВТ, что позволяет поставить вопрос о совершенствовании квалификации преступлений и рассматривать использование ВТ в качестве отягчающего обстоятельства. Третьей особенностью является «инновационность» преступности в сфере ВТ, использование не известных ранее схем совершения преступлений, что обусловлено естественной новизной самих технологий.

Таким образом, можно обозначить ряд проблем, требующих безотлагательного решения. Среди них мы выделяем:

1. Необходимость нормативного закрепления понятия «высокая технология». Основной признак ВТ – их сложность и оригинальность, недоступность для воспроизведения без специальных знаний, инструментов, материалов, а также, как правило, без глубокого разделения труда специалистов разного профиля.

2. Совершенствование, наработка методик расследования и квалификации преступлений в сфере ВТ.

3. Формирование системы упреждающего реагирования и профилактики на вероятные угрозы для общества при совершении преступлений в сфере ВТ.

Традиционные подходы к организации раскрытия и расследования преступлений нуждаются в пересмотре в связи со спецификой современных ВТ, которые появились в результате перехода общества в новую стадию развития – так называемую информационную цивилизацию.

Очевидно, что оперативная работа сегодня, как правило, не проводится без использования в той или иной степени технических средств, информационных систем и т. д. Арсенал современного оперативника несравненно богаче, чем у его коллеги, например, в XIX в., когда был сформирован классический образ сыщика.

В этой связи можно было бы предположить, что эффективность, показатели работы современного оперативного работника должны быть выше, чем 100, 50 или даже 20 лет назад. Однако этого не наблюдается. Более того, если исходить из соотношений общей численности оперативных работников (с учетом специалистов по отдельным видам ОРД) к количественным показателям эффективности, получатся обратные зависимости.

Дело в том, что применение современных высокотехнологичных средств предполагает наличие специальных навыков в технической, а не гуманитарной (юриспруденция, психология и т. д.) сфере, то есть человек должен сочетать в себе оба качества, традиционно считающие-