

ПРОБЛЕМЫ КАДРОВОЙ ПОЛИТИКИ В ПРОФИЛАКТИКЕ И ПРЕДУПРЕЖДЕНИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В КЫРГЫЗСТАНЕ

Новизна возникших проблем, процессов компьютеризации кыргызского общества, оказавшегося неготовым к активной борьбе с таким новым преступным явлением, как компьютерные преступления, требует незамедлительного решения вопроса.

Положение с научными разработками по этим проблемам, особенно в области криминалистической науки, а также практики, методики, соответствующего технического оборудования для экспертизы, слежения и т.д. для работников следственных служб совершенно отсутствует. Нет специалистов, подготовленных в этом направлении.

Остается нерешенным и ряд основных организационных аспектов, связанных, например, с координацией усилий различных государственных органов, подготовкой и переподготовкой кадров для работы с автоматизированными информационными системами и т.д.

Работа по раскрытию и расследованию компьютерных преступлений обладает целым рядом особенностей и требует специальной подготовки сотрудников правоохранительных органов.

Как свидетельствует зарубежный опыт и показывает практика расследования компьютерных преступлений, прежде всего сам следователь должен обладать определенными познаниями и навыками в этой области (знать терминологию, составные части компьютерной системы и сетей, общий режим их функционирования, основные нормативные документы, регламентирующие этот режим, правовые акты, определяющие статус машинной информации и иных информационных ресурсов, обладать навыками пользователя ЭВМ и т.д.), поскольку без этого невозможно полное и объективное расследование уголовных дел данной категории.

В свою очередь конкретная следственная ситуация обуславливает основные направления следствия, в частности, те следственные версии, которые она порождает и проверка которых требует проведения сугубо определенных следственных или оперативно-розыскных действий, что опять таки приводит к типизации операций по выявлению, исследованию и использованию разнообразной криминалистической информации, которую можно обрабатывать с использованием компьютерной техники.

В условиях роста преступности, а главное ее латентности, раскрываемость преступлений ставит задачу повышения требований к доказыванию вины обвиняемых. Экстенсивный путь наращивания сил и средств не даст никакого результата. Усложнение процесса расследования предъявляет совершенно иные, гораздо более высокие требования, прежде всего к мыслительной деятельности. Данный вид деятельности, в свою очередь, требует высочайшей квалификации, большого опыта. Специфические условия, в которых осуществляется процесс раскрытия и расследования компьютерных преступлений, обуславливает существенные изменения в организации решения задач с использованием компьютерной техники.

Отсутствие на любой стадии предварительного следствия, вплоть до его окончания, достаточно полных и достоверных данных об обстоятельствах, подлежащих обязательному установлению и составляющих в силу уголовно-процессуального закона предмет доказывания, требует совершенно новых, более оперативных и гибких подходов с использованием ПК в ходе расследования преступлений.

Используемые и разрабатываемые в настоящее время в органах внутренних дел и прокуратуры программные средства позволяют формулировать рекомендации для сложных ситуаций, возникающих в процессе расследования преступлений, подходов и методов по каждому возникшему факту индивидуально. Однако эффективность их использования ограничивается потребностью в огромных объемах информации, криминалистических, уголовно-правовых и уголовно-процессуальных знаниях, нуждающихся в формализации и введении в память указанных систем. С другой стороны, опыт использования таких систем свидетельствует о том, что является универсальным, и поэтому может быть использован при расследовании различных категорий преступлений

этого вида.

Эффективность будет зависеть от ряда рассмотренных в работе объективных и субъективных обстоятельств, из которых на первое место выступает образование, практические знания специалистов в правоохранительных органах.

Следовательно, создание общего организационно-методического центра, который координировал бы всю работу в этом направлении, наделенного соответствующими полномочиями и способного по своему профессиональному составу заниматься всеми проблемами, связанными с компьютерной преступностью, как никогда актуальна.

Несмотря на свой подфункциональный характер, правильно построенная кадровая политика способна дать значительный эффект в снижении латентности преступлений, связанных с компьютерами и важной информацией.

В числе прикладных мер, составляющих кадровую политику в целом, нам видится:

- разработка системы единой автоматизированной информационной среды;
- разработка инструктивно-методических материалов по вопросам эффективного применения информационно-вычислительных ресурсов для решения конкретных задач, поставленных перед правоохранительными органами МВД и прокуратуры;
- подготовка и введение в действие ведомственных нормативных актов, регламентирующих работу пользователей и эксплуатационного персонала единой автоматизированной информационной среды правоохранительных органов и органов прокуратуры;
- создание периодической системы подготовки и переподготовки кадров для работы с автоматизированными информационными системами, с базовыми специализированными лабораториями, снабженными техникой и специальной технологией;
- создание автоматизированного рабочего места (АРМ) по каждому виду деятельности органов прокуратуры, т.е. создание локальной问题导向ной базы данных и программно-технических средств (ПТС) для решения определенной логической полной группы задач по направлению деятельности (например, АРМ следователя);
- объединение локальных баз данных на каждом из уровней управления в интегрированный банк данных с возможностью его коллективного использования;
- обеспечение оперативного удаленного доступа к базам данных (локальным и интегрированным) непосредственно с рабочих мест сотрудников в соответствии с их компетенцией, т.е. с учетом разграничения доступа;
- разработка многоуровневых специализированных информационных систем для оперативных служб Генеральной прокуратуры и правоохранительных органов с возможностью обмена информацией по выделенным каналам связи по вертикали и горизонтали от Генеральной прокуратуры до районных, такая же вертикаль и горизонталь и в правоохранительных органах;
- объединение вычислительных и информационных ресурсов правоохранительных органов и прокуратуры в единую информационно-вычислительную сеть, далее (ИВС) – прокуратура и т.д. с адаптацией к существующей информационной инфраструктуре;
- обеспечение информационного взаимодействия с автоматизированными информационными системами и базами данных, создаваемыми в высших органах государственной власти и управления, министерствах и ведомствах правовой сферы, других министерствах и ведомствах (Госкомстат и др.);
- типизация и унификация проектных решений (информационных, технических, программных, технологических) в целях их последующего массового применения в соответствующих органах и удешевления за счет этого всей системы информатизации;
- обеспечение лицензионной чистоты технических средств и программных продуктов для создания открытых информационных систем, соответствующих международным стандартам защиты интеллектуальной собственности;
- обеспечение защиты информации в базах данных различных уровней от несанкционированного доступа, копирования, искажения и разрушения;
- обеспечение надежности (достоверности) и функциональной полноты информации, хранящейся в базах данных различных уровней вплоть до их сертификации

на государственном уровне;

Далее считать не менее важным учет следующих моментов при подборе кадров:

- всесторонне изучать лиц, изъявивших желание работать со специалистами с целью выявления среди них тех, кто ранее допускал правонарушения или предрасположен к ним;
- при отборе кандидатов на работу в зависимости от степени риска проделать особо тщательный отбор кандидатур;
- периодически проводить ротацию сотрудников, позволяющую оценить их поведение с точки зрения обеспечения безопасности;
- обучение персонала теоретически и практически правилам защиты данных от несанкционированного доступа и других видов преступлений данного рода с учетом последних нововведений; командировки в другие страны с целью обмена опытом;
- осуществление систематического контроля за деятельностью сотрудников.

Литература:

1. Конституция КР. -Б.: Госконцерн «Учкун», 1996.
2. Уголовный Кодекс КР (от 1 октября 1997 г.). - Б.: «НАКР», 1997. - 168 с.
3. Гоценко О.Ю. Защита информации. - Санкт-Петербург: Изд. Дом «Сентябрь», 2001. – 228 с.
4. Ярочкин В.И. Информационная безопасность. - М.: Летописец, 2000.