**КОНТРОЛЬНАЯ РАБОТА**

**по курсу «Государственное право»**

**1. Информационные технологии оперативно-розыскной деятельности**

Повышение эффективности деятельности правоохранительных органов по раскрытию, расследованию и предупреждению преступлений невозможно без внедрения современных информационных технологий. В процессе раскрытия, расследования и предупреждения преступлений применяется как универсальное, так и специальное программное обеспечение. В частности, к универсальным программам общего назначения относятся:

а) системы подготовки текстов, предназначенные для набора и редактирования документов;

б) универсальные программы управления базами данных, перерабатывающие большое количество однотипной информации и систематизирующие ее по нужным признакам;

в) электронная таблица – электронный банк, в ячейки которого можно заносить не только текстовые символы, но и математические формулы, при этом расчеты производятся автоматически;

В настоящее время можно выделить следующие основные направления разработки и применения компьютерных технологий в оперативно-розыскной деятельности:

1) автоматизация системы уголовной регистрации;

2) компьютеризация процесса расследования преступлений;

3) автоматизация процесса производства экспертиз и исследований.

В системе уголовной регистрации сосредоточен значительный объем информации, используемой правоохранительными органами в процессе раскрытия, расследования и предупреждения преступлений. В этой связи повышение оперативности и эффективности обработки и выдачи информации находится в прямой зависимости от внедрения современных компьютерных технологий. Можно констатировать, что данной проблеме уделяется весьма существенное внимание. Так, в Главном управлении по борьбе с контрабандой Государственного таможенного комитета РФ разработана информационно-поисковая система «БК-ИНФОРМ» с целью информационной поддержки расследований по делам о нарушении таможенных правил, производства дознания по уголовным делам, проведения оперативно-розыскной деятельности, в том числе и деятельности, связанной с борьбой с контрабандой и нарушениями таможенных правил. Круг задач системы «БК-ИНФОРМ» достаточно обширен: собирание, обработка, хранение и выдача информации по делам о таможенных правонарушениях; уголовным делам; о контрабанде наркотических веществ, особо опасным видам контрабанды; информационное обеспечение оперативно-розыскной деятельности оперативных подразделений и органов дознания; нормативно-правовое обеспечение правоохранительной деятельности; интеграция информации, получаемой при решении задач «БК-ИНФОРМ» для использования в правоохранительной деятельности таможенных органов.

Система содержит значительный объем сведений о личности правонарушителей в таможенной сфере, поскольку подсистемы «Производство по делам о НТП» и «Дознание по уголовным делам» содержат базы данных о лицах, совершивших указанные правонарушения. В настоящее время система «БК-ИНФОРМ» проходит опытные испытания. В стадии экспериментальной проверки находится и другая информационно-поисковая система «Информационная поддержка оперативно-розыскной и следственной деятельности», также содержащая сведения о лицах, совершивших правонарушения в таможенной сфере.

Значительное внимание уделяется компьютеризации системы уголовной регистрации МВД РФ, насчитывающей свыше 50-ти различных учетов. В частности, в централизованном автоматизированном учете особо опасных (квалифицированных) преступников (рецидивисты, гастролеры, организаторы преступных групп, авторитеты уголовной среды) накопление и обработка информации осуществляется с помощью подсистемы «Досье». Подсистема «Досье» информационно связана с центральной фототекой, в которой хранятся фотографии лиц, поставленных на учет. Фототека информационно может быть периодически связана с централизованной видеотекой (видеозаписями лиц).

В состав АИС «Криминал-И», которая используется для ведения учета правонарушений и преступлений, совершенных иностранными гражданами, лицами без гражданства (ЛБГ) и гражданами России, постоянно проживающими за границей, функционируют пять автоматизированных подсистем:

«Автоматизированная практика» («Адмпрактика»);

«Преступление»;

«Дорожно-транспортное происшествие» («ДТП-И»);

«Розыск»;

«Наказание».

Так, в частности, подсистема «Розыск» предназначена для информационного обеспечения заинтересованных служб оперативно-справочной и аналитической информацией об иностранцах и ЛБГ, находящихся в розыске и разысканных. Эта подсистема не изменяет существующий в настоящее время порядок информирования об их розыске, а лишь в целях оперативности дополняет его автоматизированным контуром.

В рамках Федеральной пулегильзотеки ЭКЦ МВД РФ функционируют информационно-вспомогательные автоматизированные системы:

«Клеймо» – маркировочные изображения и клейма охотничьего нарезного оружия и припасов к нему;

«Пламя» – тактико-технические характеристики, разборка и сборка деталей, маркировочные обозначения, внешний вид автоматических пистолетов отечественного и импортного производства;

«Боеприпасы» – изображение, характеристики и маркировочные изображения;

«Оружие» – описание (без изображения) и характеристики автоматических пистолетов, автоматов и карабинов;

«Ружье» – изображение, тактико-технические характеристики, маркировочные обозначения отечественного охотничьего и спортивного оружия;

«Патрон» – изображение, тактико-технические характеристики, маркировочные обозначения, особенности заряда патронов к охотничьим ружьям отечественного производства.

Продолжается эксплуатация ныне функционирующей системы автоматизированных банков данных (АБД). Она является универсальной и функционирует в двух уровнях: общероссийском (АБД «Центр») и региональном (АБД «Республика Область»).

АБД «Республика Область» включает сведения:

а) об особо опасных рецидивистах; лицах, осужденных к лишению свободы за тяжкие преступления или осужденных два или более раза за любые умышленные преступления, либо ранее освобожденные из мест лишения свободы до полного отбытия назначенного наказания и вновь совершивших преступления;

б) о нераскрытых преступлениях по способу совершения и сокрытия похищенных вещей;

в) о предметах, вещах, имеющих индивидуальные номера или характерные особенности, похищенных, изъятых у задержанных и арестованных; похищенных, выявленных предметах антиквариата;

г) о похищенных, угнанных и не разысканных АМТ средствах;

д) о похищенном, утерянном, изъятом, найденном и добровольно сданном огнестрельном оружии, боеприпасах, взрывчатых веществах.

АБД «Центр» включает сведения:

о лицах, ранее судимых к лишению свободы за тяжкие преступления;

о нераскрытых особо опасных преступлениях, а также преступлениях на междугороднем транспорте;

о похищенных и изъятых у преступников предметов, имеющих индивидуальные номера или характерные признаки;

о произведениях изобразительного искусства и антиквариата;

об угнанных, найденных у преступников и изъятых АМТ средствах;

о похищенном и изъятом огнестрельном оружии;

о наркотических и других сильнодействующих лекарственных веществах, имеющих маркировку.

Одно из перспективных направлений компьютеризации процесса расследования – разработка информационно-поисковых систем по установлению личности преступника при расследовании конкретных уголовных дел. Использование таких систем основано на информации, полученной при выявлении взаимосвязей, по расследованным уголовным делам, между свойствами преступника и остальными элементами преступной деятельности.

**2. Компьютерные вирусы и антивирусные средства**

С увеличением количества людей, пользующихся компьютером, и возможностей обмена между ними данными по электронной почте и через интернет возросла угроза заражения компьютера вирусами, а также порчи или хищения информации прочими вредоносными программами.

В целом вредоносные программы можно разделить на следующие три класса:

* Черви – данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения.

Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

* Вирусы – программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение. Скорость распространения вирусов несколько ниже, чем у червей.
* Троянские программы – программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

В последнее время наиболее распространенными типами вредоносных программ, портящими компьютерные данные, стали черви. Далее по распространенности следуют вирусы и троянские программы. Некоторые вредоносные программы совмещают в себе характеристики двух или даже трех из перечисленных выше классов.

Основными источниками распространения вредоносных программ является электронная почта и интернет, хотя заражение может также произойти через дискету или CD-диск. Это обстоятельство предопределяет смещение акцентов антивирусной защиты с простых регулярных проверок компьютера на присутствие вирусов на более сложную задачу постоянной защиты компьютера от возможного заражения.

Антивирусная программа (антивирус) предназначена для защиты компьютеров от большинства вирусов, червей и «троянских коней», которые могут удалить файлы, получить доступ к личным данным либо использовать зараженную систему как средство атаки на другие компьютеры. Антивирусная программа может быть предварительно установлена на компьютер, а может быть приобретена и установлена самостоятельно.

Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

К сожалению, конкуренция между антивирусными компаниями привела к тому, что развитие идёт в сторону увеличения количества обнаруживаемых вирусов (прежде всего для рекламы), а не в сторону улучшения их детектирования (идеал – 100%-ое детектирование) и алгоритмов лечения заражённых файлов.

Антивирусное программное обеспечение состоит из компьютерных программ, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы. Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

1. Просмотр (сканирование) файлов для поиска известных вирусов, соответствующих определению в словаре вирусов.

Это метод, когда антивирусная программа, просматривая файл, обращается к словарю с известными вирусами, который составлен авторами программы-антивируса. В случае соответствия, какого либо участка кода просматриваемой программы известному коду вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий:

Удалить инфицированный файл.

Отправить файл в карантин (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).

Попытаться восстановить файл, удалив сам вирус из тела файла.

Для достижения достаточно продолжительного успеха, при использовании этого метода необходимо периодически пополнять словарь известных вирусов новыми определениями (в основном в онлайновом режиме).

Антивирусные программы, созданные на основе метода соответствия определению вирусов в словаре, обычно просматривают файлы тогда, когда компьютерная система создаёт, открывает, закрывает или посылает файлы по электронной почте. Таким образом, вирусы можно обнаружить сразу же после занесения их в компьютер и до того, как они смогут причинить какой-либо вред. Надо отметить, что системный администратор может составить график для антивирусной программы, согласно которому могут просматриваться (сканироваться) все файлы на жёстком диске.

2. Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается записать какие-то данные в исполняемый файл (exe-файл), программа-антивирус может пометить этот файл, предупредить пользователя и спросить что следует сделать.

В отличие от метода соответствия определению вируса в словаре, метод подозрительного поведения даёт защиту от совершенно новых вирусов, которых ещё нет ни в одном словаре вирусов. Однако, программы, построенные на этом методе, выдают также большое количество ошибочных предупреждений, что делает пользователя мало восприимчивым ко всем предупреждениям. Если пользователь нажимает мышью на окно «Принять» («Accept») в каждом случае появления такого предупреждения, антивирусная программа не приносит никакой пользы. В последнее время эта проблема ещё более ухудшилась, так как стало появляться всё больше невредоносных программ, модифицирующих другие exe-файлы, несмотря на существующую проблему ошибочных предупреждений. Таким образом, в современном антивирусном программном обеспечении этот метод используется всё меньше и меньше.

3. Другие методы обнаружения вирусов

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы, перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет себя как вирус (то есть немедленно начинает искать другие exe-файлы, например), такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

Ещё один метод определения вирусов включает в себя использование «песочницы». Песочница имитирует операционную систему и запускает исполняемый файл в этой имитируемой системе. После исполнения программы, антивирусное программное обеспечение анализирует содержимое песочницы на присутствие каких либо изменений, которые можно квалифицировать как вирус. Из-за того, что быстродействие системы снижается и требуется достаточно продолжительное время для выполнения программы, антивирусные программы, построенные по этому методу, обычно используются только для сканирования по запросу пользователя. Следует отметить, что эффективность данных программ намного выше, чем у всех остальных, но и стоимость их тоже выше. Из-за большого времени таких выполнения программ, они не найдут широкого распространения среди рядовых пользователей. Несомненно, эти программы представляют интерес для профессионалов, занимающихся вопросами компьютерной безопасности и восстановлением данных после несанкционированного доступа в компьютер пользователя или атак на сервер.

**3. Электронная почта Интернет**

E-mail (Electronic mail) – электронная почта – электронный аналог обычной почты. Стандартный сервис Internet, реализующий аналог обычной почты; предоставляет полный спектр возможностей, доступных при пользовании обычной почтой, а также множество дополнительных удобств. E-mail превосходит обычную почту по скорости на несколько порядков. Во всех отношениях удобнее и предпочтительнее традиционной. Единственный ее недостаток – слабая конфиденциальность, что, впрочем, также преодолимо благодаря возможности шифровать сообщения.

С помощью электронной почты можно посылать сообщения, получать их в свой электронный почтовый ящик, отвечать на письма корреспондентов автоматически, используя их адреса, исходя из их писем, рассылать копии писем сразу нескольким получателям, переправлять полученное письмо по другому адресу, использовать вместо адресов (числовых или доменных имен) логические имена, создавать несколько подразделов почтового ящика для разного рода корреспонденции, включать в письма текстовые файлы, пользоваться системой «отражателей почты» для ведения дискуссий с группой корреспондентов и т.д. Из Internet можно посылать почту в сопредельные сети, если известен адрес соответствующего шлюза, формат его обращений и адрес в той сети.

Для каждого абонента на одном из сетевых компьютеров выделяется область памяти – электронный почтовый ящик. Доступ к этой области памяти осуществляется по адресу, который сообщается абоненту, и паролю, который абонент придумывает сам. Пароль известен только абоненту и сетевому компьютеру. Став абонентом компьютерной сети и получив адрес своего почтового ящика, пользователь может сообщить его друзьям, знакомым. Каждый абонент электронной почты может через свой компьютер и модем послать письмо любому другому абоненту, указав в послании его почтовый адрес.

Все письма, поступающие на некоторый почтовый адрес, записываются в выделенную для него область памяти сетевого компьютера. Сетевой компьютер (или сервер), содержащий почтовые ящики абонентов, носит название хост-компьютера (от host – хозяин). Абоненты периодически скачивают с сервера поступившие для них почтовые сообщения.

E-mail дает возможность проводить телеконференции и дискуссии. Для этого используются, установленные на некоторых узловых рабочих машинах, mail reflector-ы. (списки рассылки). Туда отсылается сообщение с указанием подписать на такой-то рефлектор (дискуссию, конференцию, и т.д.). После этого начинают приходить копии сообщений, которые туда посылают участники обсуждения. Рефлектор почты просто по получении электронных писем рассылает их копии всем подписчикам.

Пересылать по e-mail можно и двоичные файлы, не только текстовые. В UNIX, например, для этого используется программы UUENCODE и UUDECODE. С введением стандарта MIME («Multipurpose Internet Mail Extensions» – Многоцелевые расширения почтового стандарта Internet) возможности электронной почты значительно расширены – в одном сообщении можно передавать множество бинарных и текстовых данных, даже с HTML разметкой.

Скорость доставки сообщений электронной почты сильно зависит от того, каким образом она передается. Путь электронного письма между двумя машинами, непосредственно подключенными к Интернет, занимает секунды, и при этом вероятность потери или подмены письма минимальна. С другой стороны, если для передачи электронных писем используются технологии FTN (последовательной передачи файлов многими компьютерами по цепочке), и письмо посылается в какую-нибудь экзотическую сеть, то письмо, во-первых, будет идти долго – дни и даже недели, во-вторых, будет иметь большие шансы просто потеряться при обрыве связи во время передачи по цепочке, в-третьих, его могут легко подменить где-то в пути следования.

В Internet наиболее часто используется несколько протоколов для передачи почты:

SMTP (Simple Mail Transfer Protocol) − только отправлениесообщений;

Широко используется в сети Internet для обмена корреспонденцией между почтовыми ящиками серверов и их клиентов. Поставщик услуг Internet предоставляет необходимое название сервера, порт, имя пользователя и пароль для доступа к SMTP-серверу.

POP3 (Post Office Protocol Version 3) − отпpавление/получение сообщений;

Особенность протокола − получение почты происходит по запросу клиента. Поставщик услуг Internet предоставляет необходимое имя сервера, порт, имя пользователя и пароль, необходимые для доступа на POP3 сервер.

IMAP4 (Internet Message Access Protocol) − это метод доступа к электронной почте или электронным доскам объявлений, хранящемся на почтовом сервере;

Другими словами, он дает клиентской почтовой программе возможность удаленного доступа к почте, как если бы она хранилась локально. Например, с почтой, размещенной на IMAP сервере, можно работать с домашнего персонального компьютера, с рабочей станции из офиса, с ноутбука во время путешествия, что не требует перекачивания информации между этими компьютерами.

IMAP4 представляет собой надмножество POP3, обладающее расширенными возможностями. Он обеспечивает поддержку всех типов удаленного доступа к почтовым ящикам: автономный и on-line. Аутентификация для IMAP серверов работает, так же как и для POP3.

**4. Бланки сообщений**

Бланки сообщений – важная часть электронной почты. Непосредственно в них набирается текст письма. Приведем небольшой пример:

Создать и отправить письмо в почтовой программе The Batдля адресата test@test.com. К письму присоединить файл c:\student\test.txt.

1. Выбираем пункт меню «Письмо → Создать» или нажимаем Ctrl+N.

2. В поле «Кому» указываем test@test.com, в поле «Тема» – тему письма (например, «Проверка»), в области для текста письма набираем с клавиатуры сообщение для адресата.

3. Кликаем мышью по кнопке «Прикрепить файл» (или нажимаем Alt + Page Up). В появившемся диалоге открытия файла находим и выбираем файл

c:\student\test.txt.

4. Кликаем мышью по кнопке «Отправить письмо» или нажимаем F2.

Важной частью бланка сообщения является адрес электронной почты. Адрес электронной почты, так же как и обычный почтовый адрес должен содержать всю необходимую информацию для того, чтобы письмо дошло до адресата из любой части земного шара. Точно так же, как и почтовый, электронный адрес состоит из двух частей:

раздел «Куда» – содержит указание на хост-компьютер;

раздел «Кому» – содержит учетное имя абонента.

В разных системах используются различные способы представления адреса. Например, в системе INTERNET и совместимых с ней разделы «Кому» и «Куда» разделены знаком «@», причем слева указывается «Кому». Например:

user@adonis.iasnet.ru,

где user – учетное имя абонента, а adonis.iasnet.ru – имя хост-компьютера

(adonis) и указание, как его найти. Раздел «Куда» имеет иерархическую

структуру. Уровни иерархии называются доменами (domain – владение, сфера деятельности) и разделены точками. Количество доменов в адресе, вообще говоря, не ограничено. Самый правый домен представляет собой домен верхнего уровня. В данном случае, ru – код России. Для всех стран существуют двухбуквенные коды. Например :

au – Австралия,

br – Бразилия,

by – Беларусь,

ca – Канада,

cn – Китай,

de – Германия,

jp – Япония,

ua – Украина,

uk – Великобритания,

us – США.

Домен верхнего уровня не обязательно является кодом страны. Ниже приведены примеры нескольких доменов верхнего уровня, используемых в США:

COM – коммерческие организации и бизнес;

EDU – образовательные учреждения;

NET – структурные организации системы;

ORG – неприбыльные организации;

INT – международный домен.

Домен второго уровня дает уточнение для поиска хост компьютера. Это может быть код города или региона, в США – штата. В приведенном выше примере домен второго уровня указывает на компьютерную сеть Института Автоматизированных систем (iasnet).

**Список использованных источников**

1. Криминалистика./ Под ред. Ялышева С.А. М., 2004.
2. Жбанков В.А. Основные направления использования современных компьютерных технологий в криминалистике. / Ученые записки Ульяновского государственного университета. Сер. Государство и право / Вып. 1 (11). Государство и право: проблемы, поиски решений, предложения. Под ред. Чучаева А.И. – Ульяновск: УлГУ, 2000. – С. 112-116.
3. Официальный сайт программы The Bat!

http://www.ritlabs.com/ru/products/thebat/

1. Стрельцов А.А. Компьютерные антивирусные программы. М., 2004.
2. Фридланд А.Я. Информатика: Процессы, системы, ресурсы. М., 2003.