**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

 **«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ имени И.Т. Трубилина»**

ФАКУЛЬТЕТ ЮРИДИЧЕСКИЙ

**Тезисы лекций дисциплины**

**Б1.В.1.16 «Информационные технологии в юридической деятельности»**

*наименование дисциплины*

**Программа бакалавриата по направлению подготовки**

40.03.01 «Юриспруденция»

**Направленность подготовки**

гражданско-правовая

**Уровень высшего образования**

Бакалавриат

**Форма обучения**

очная, заочная

**Краснодар**

**2018**

**КОНСПЕКТ ЛЕКЦИЙ**

### 1. Понятие, задачи и система правовой информатики и кибернетики.

### *1.1. Понятие и взаимосвязь правовой информатики и кибернетики.*

Термин «информатика» возник в 60-х годах прошлого века во Франции для названия области автоматизированной обработки информации с помощью электронных вычислительных машин, слияние слов информация и автоматика и озна­чает «информационная автоматика», или «автоматизированная переработка информации».

В российской науке существуют различные точки зрения на эту проблему.

Н.С. Полевой и А.Р. Шляхов рассматривали правовую ин­форматику как одно из направлений науки кибернетики. Предме­том этого направления являются закономерности образования, восприятия, хранения, обработки и выдачи социально-правовой информации в целях повышения эффективности организационно­го взаимодействия управляющих и управляемых систем в право­вой сфере общества[[1]](#footnote-1).

Ю.М. Батурин в правовой информатике выделяет три состав­ляющих: 1) техническую сторону информационного права и про­граммное обеспечение правовых задач;

2) специализированные юридические системы и принятие юридических решений с по­мощью ЭВМ;

3) основы теории информации применительно к пра­ву[[2]](#footnote-2).

Особый интерес, на наш взгляд, представляет точка зрения Л.Б. Венгерова, который связывает предмет правовой информа­тики с «информационной концепцией права, то есть учением об информационной природе права», а информационно-правовую деятельность рассматривает как новое направление в юридиче­ской работе[[3]](#footnote-3).

Развивая эти положения, М.М. Рассолов и В.Д. Элькин опреде­ляют правовую информатику как «прикладную науку, изучающую проблемы сбора, восприятия, регистрации, хранения, обработки и использования социально-правовой информации в правовой системе общества и ее подсистемах как специфических правовых информационных образованиях»[[4]](#footnote-4).

О.А. Гаврилов, соглашаясь с предложенным Н.С. Полевым определением, определяет правовую информатику как «междис­циплинарную отрасль знаний о закономерностях и особенностях информационных процессов в сфере юридической деятельности, об их автоматизации, о принципах построения и методиках ис­пользования автоматизированных информационных систем, соз­даваемых для совершенствования и повышения эффективности юридической деятельности и решения правовых задач на базе комплексного использования теории и методологии правовых наук средств и методов математики, информатики и логики»[[5]](#footnote-5).

Анализ указанных подходов позво­ляет выделить, два наиболее важных направления.

1. Связано с исследованием правовой сис­темы общества, ее подсистем, социально-правовой информации как специфических информационных правовых образований.

2. Связано с уче­том правовых особенностей изучаемых объектов, явлений и про­цессов.

Учитывая сказанное, ***правовую информатику можно опреде­лить как науку, изучающую информацию, информационные про­цессы, информационные технологии и информационные системы в правовой сфере на основе исследования правовых особенностей изучаемых объектов, явлений и процессов.***

Наиболее тесно информатика связана с *кибернетикой* – наукой о закономерностях управления сложными динамическими системами. В качестве таких систем рассматриваются и живые организмы, и социаль­ные сообщества, и технические системы.

В 60-70 годах XX века проблемы исследования киберне­тических систем нашли широкое отражение в различных отрас­лях науки. Активно развивались и научная теория ***правовой кибер­нетики – науки, изучающей закономерности, условия и особен­ности использования математических методов и технических средств в целях оптимизации и повышения эффективности управленческих процессов при решении конкретных правовых задач.*** Сегодня правовая кибернетика активно используется при исследовании эффективности законодательного и иного правово­го регулирования общественных отношений.

Основные объекты исследования правовой кибернетики:

а) управляющее устройство – правотворческий орган, уста­навливающий нормы права, задающие поведение субъектов пра­воотношений;

б) управляемое устройство – субъекты правоотношений, ко­торым информационно-правовыми нормами предписываются определенные правила поведения (права, обязанности, ответст­венность);

в) прямая и обратная связи – каналы, по которым движется правовая информация – нормативная (как команда управления) и ненормативная (как информация обратной связи).

### *1.2. Предмет и задачи правовой информатики.*

***В предмет правовой информатики*** входит изучение информационных про­цессов, информационных отношений, информационной деятельности в правовой сфере жизни общества. Она изучает также процессы управления данной сферой.

Правовая информатика яв­ляется частью общей информатики.

***Общая информатика*** – это наука, изучающая структуру и свойства информации, а также закономерности информационной дея­тельности, ее теорию, методику и организацию.

В состав правовой информатики входят теоретическая и прикладная информатика.

***Теоретическая информатика*** изучает общие закономерности информационных процессов и их математические модели.

***Прикладная информатика*** ориентирована на применение средств автоматизации для решения практических задач. Отраслевые направления информатики имеют своей целью изучение информационных процессов в конкретных науках (экономика, социология, право и др.).

***Целью правовой информатики*** является раз­работка оптимальных способов и средств представления, сбора, аналитической переработки, хранение, поиска и распространение информации в процессе юридической деятельности.

Важнейшими ***задачами правовой информатики*** являются:

- исследование и разработка теории правовой информа­ции и методологических основ ее подготовки к машинной обработке (данная задача включает в себя: сущ­ность правовой информации, её значение, виды, источ­ники и носители; методы собирания и анализа правовой ин­формации; формализация, метризация и иные способы ее подготовки к машинной обработке);

- исследование и разработка технологии обработки пра­вовой информации и решение правовых задач с использо­ванием средств вычислительной техники (данная задача включает в себя: ЭВМ, как средство обработки и хра­нения правовой информации; алгоритмическое и программное обеспечение работы ЭВМ; особенности постановки и реше­ния правовых задач с использованием ЭВМ);

- исследование и разработка частных методик решения правовых задач на основе использования идей, средств и методов математики, логики, информатики, кибернетики и сопряженных с ними наук;

- исследование и разработка теоретических основ, принципов построения и практики использования автома­тизированных информационных систем и комплексов для решения правовых задач в различных отраслях юридиче­ской деятельности (АИПС, АИЛС, АСУ, АОС).

### *1.3. Связь правовой информатики и кибернетики с другими науками.*

В рамках правовой информатики осуществляется синтез данных юридиче­ских и иных общественных, технических, естественных и математических наук. Вместе с тем данная отрасль знаний принадлежит к системе юридического знания, ибо в ее основе лежат фундаментальные юридические представления и факты.

Связь правовой информатики с ***техническими науками*** реализуется по линии активного использования для нужд юридической науки и практики современных ЭВМ различных классов. В свою очередь использование ЭВМ опирается на вовле­чение в сферу интересов правовой информатики возможностей формальной логи­ки и математики, без чего невозможна формализация правовых норм перед введе­нием их в память ЭВМ.

Большое значение имеет использование в правовой информатике достиже­ний ***общей теории права.*** Процесс информатизации должен опираться на научные представления о государстве и праве. Источни­ком этих представлений является общая теория права, и прежде всего такие ее по­ложения, которые касаются общих принципов протекания информационных про­цессов, критериев правовой информированности, соотношения информирован­ности граждан и уровня их правовых знаний и других теоретических положений. Процесс информатизации правовой сферы жизни общества опирается на такие понятия общей теории права, как право и законодательство, законодательство и отрасль законодательства, правовая система и д.р.

Правовая информатика тесно связана с **наукой конституционного права.** Это следует из того, что в Конституции РФ закреплены основные нормы, оказы­вающие значительное воздействие на формирование и развитие информационных отношений. Так, согласно ч. 4 ст. 29 Конституции, каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Конституция вводит понятие информации о частной жизни граждан, о ма­териалах и документах государственных органов, а также понятие о государствен­ной тайне, как разновидности информации с особым режимом. Конституция со­держит важные нормы, регламентирующие порядок реализации права на инфор­мацию.

Проблемы, связанные с получением и аналитической обработкой информа­ции, возникают во всех юридических науках. Каждая юридическая наука должна создавать информационную модель объекта своего познания, что предполагает активное использование методов и средств общей и правовой информатики. При создании автоматизированных информационно-поисковых систем по законода­тельству необходимо использовать классификацию нормативных правовых актов (НПА), которые содержатся в отраслевых юридических науках (уголовное право, гражданское право, административное право и др.).

### *1.4. Методология правовой информатики и кибернетики.*

***Методология науки*** это учение о постижении истины, об ее использовании, о методах движения знания к производству и к иным сферам практической деятельности.

***Метод*** это совокупность требований, ориентирующих субъекта в его познавательной деятельности, в частности, применительно к выбору способа, средства и необходимых операций, которые должен совершить субъект деятельности, чтобы достичь поставленной цели.

Специальными методами исследования данной науки являются методологические подходы. Рассмотрим наиболее распространенные из них:

***1. Системно-структурный подход*** – отталкиваясь от отдельных элементов и выполняемых системных функций, анализируется только структура системы и взаимосвязи элементов, относящихся к ней.

***2. Функциональный подход*** – абстрагируясь от содержания отдельных элементов системы их взаимосвязи и общей структуры, анализируется только функции, присущие той или иной системе в целом.

***3. Алгоритмический подход*** – (алгоритм – совокупность операций, необходимых для решения задачи, выполняемых в определенном порядке) требует не только анализа структуры системы и выполняемых ею функций, но и уяснение того, какие операции и в какой последовательности система выполняет, чтобы наиболее оптимально решать поставленные задачи.

***4. Моделирование***– под моделированием понимается исследование кибернетических процессов, явлений, систем объектов путем построения и изучения их моделей, каждая из которых отображает или воспроизводит объект-оригинал, способна заменить его так, что её изучение дает новую информацию об этом объекте. Специфичность этого метода познания состоит в том, что в результате моделирования создается промежуточный элемент познания – модель, которая в познавательном процессе выполняет следующие функции:

- замещение моделируемого объекта;

- информационную;

- гносеологическую;

- формализационно-алгоритмическую;

- доказательственно-иллюстративную.

Моделирование имеет несколько видов:

- предметное или материально-реализованное;

- логико-материальное (явления, процессы, последовательность);

- кибернетическое (с использованием ЭВМ);

- мысленное (создание образа).

### *1.5. Система правовой информатики и кибернетики.*

Предмет и задачи правовой информатики и кибернетики обуславливают ее систему.

Она состоит из общей и особенной частей.

***Общая часть***носит теоретический характер и включает в себя:

- Понятие, задачи и систему правовой информатики и кибернетики;

- Основные понятия правовой ПИиК и их значение (информация, правовая информация, система, информационная система, информационные процессы, информационные технологии, управление системой);

- Правовое регулирование в сфере информационных процессов;

- Подготовку правовой информации к машинной обработке;

- Автоматизированные системы правовой информации: автоматизированные информационно поисковые системы (АИПС); автоматизированные информационно-логические системы (АИЛС); автоматизированные системы управления (АСУ); автоматизированные обучающие системы (АОС);

- Компьютеризацию правотворческой и правоприменительной деятельности.

***Особенная часть***изучает использование кибернетических средств и методов в различных видах правоохранительной и юридической деятельности, а также понятие и защиту от компьютерных преступлений. Она носит как бы прикладной характер и включает в себя.

Использование INTERNET в профессиональной деятельности юриста.

Общеюридические информационные системы «РАСИНА», «КОНСУЛЬТАНТ-ПЛЮС», «КОДЕКС», «ГАРАНТ», «ЮСИС».

Использование ЭВМ в организации и методике расследования преступлений.

Автоматизацию криминалистических учетов;

Компьютеризацию судебной экспертизы;

Криминальную деятельность в области информационных отношений;

Защиту от компьютерных преступлений;

Электронная цифровая подпись.

### 2. Основные понятия правовой информатики и кибернетики их значение.

### *2.1. Понятие информации и её виды.*

Современный этап развития человечества характеризуется движением от промышленного общества к обществу информационному через информатизацию всех областей и направлений деятельности.

Остановимся на наиболее известных определениях понятия информации, изложенных известными учеными, стоящими у истоков возникновения теории информации.

Информация – это содержание, полученное из внешнего мира (Ноберт Винер);

Информация – это уменьшаемая, снимаемая неопределённость в результате получения сообщений (Шеннон);

Информация – это передача разнообразия (Эшби);

Информация – это оригинальность, новизна (Моль);

Информация – это вероятность выбора (Яглом);

Информация – это отраженное разнообразие (Урсул).

Впервые в России на законода­тельном уровне официально определение понятия информации было дано в Федеральном законе от 20 февраля 1995 г. «Об информации, информатизации и защите информации». В соот­ветствии со ст. 2 Закона: информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Вместе с тем выработать об­щее определение понятия информации не удалось.

На наш взгляд, ***информация – это разнообразные сведения, факты, данные о явлениях и процессах, происходящих в природе и обществе, в технических устройствах и жи­вых организмах. Понятие информации тесно связано с понятиями сообщения, сиг­нала, сложности, структуры и разнообразия.***

Различают следующие ***виды информации*.**

По сфере применения:

- массовая;

- правовая;

- научно-техническая;

- политическая;

- социальная;

- статистическая;

- о гражданах (персональные данные).

***По режимам доступа:***

- открытая (общедоступная);

- ограниченного доступа (государственная тайна, конфиденциальная информация).

***По видам носителей:***

- на бумаге;

- на машиночитаемых носителях;

- в виде изображения на экране ЭВМ;

- в памяти ЭВМ;

- передаваемая по каналам связи;

- на других носителях.

***Информация о гражданах*** (персональные данные) введено Законом об информации. Информация о гражданах – это сведения о фактах, событиях и обстоятельствах жизни гражда­нина, позволяющие идентифицировать его личность (ч. 6 ст. 2). Основными эле­ментами информации о гражданах являются имя и фамилия, пол, дата и место рождения, место проживания, образование и семейное положение.

Понятие***компьютерной информации***введено Уголовным кодексом РФ 1996 г., в ст. 272 которого дано определение этого вида информации, как ин­формации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или в их сети.

***Научно-техническая информация***представляет собойдокументированные или публично оглашаемые сведения об отечественных и зару­бежных достижениях науки, техники и производства, полученные в ходе научно-исследовательской, опытно-конструкторской, проектно-технологической, произ­водственной и общественной деятельности.

***Документированная информация***(документ) это зафиксированная на материальном носителе информация с рек­визитами, позволяющими ее идентифицировать (ч. 4 ст. 2 Закона об информации).

***Государственная тайна***представляет собойзащищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб без­опасности Российской Федерации (ст. 2 Закона РФ «О государственной тайне» от 24 июля 1993г.).

Государственная тайна относится к информации ограниченного пользова­ния. Допуск к ней осуществляется путем оформления права граждан на получение сведений, составляющих государственную тайну.

***2.2. Правовая информация.***

Правовая информация это сведения о фактах, событиях, предметах, лицах, явлениях, протекающих в правовой сфере жизни общества, содержащихся как в нормах права, так и в других источниках, и используемая государством и обществом для решения правотворчества, правоприменительной и правоохранительной деятельности, защиты прав и свобод личности.

***Требования, которые предъявляются к правовой информации***, могут быть сформулированы следующим образом:

- правовая информация должна быть достоверной, т. е. объективно отражать реальность;

- она должна быть полной, т. е. отражать все относящиеся к данному случаю факты, явления, процессы.

Правовая информация делится на нормативную правовую информацию и ненормативную правовую информацию.

***Нормативная правовая информация*** является совокупностью официальных документированных данных о праве и законода­тельстве, их системе, источниках, отдельных правовых нормах и правовых инсти­тутах, юридически закрепляющих правовые отношения между физическими и юридическими лицами и иными субъектами российского права.

К ***источникам нормативной правовой информации*** относятся законодатель­ные и иные нормативные правовые акты, международные договоры и соглашения, общепризнанные нормы и принципы международного права. Сюда же относятся толкование правовых норм и обобщение правовой практики (например, судебной).

Нормативная правовая информация может быть классифицирована следующим образом:

1) информация, содержащаяся в Конституции РФ, в федеральных конститу­ционных и федеральных законах, указах Президента РФ, постановлениях и распо­ряжениях правительства, актах министерств и ведомств, актах органов законода­тельной и исполнительной власти субъектов Российской Федерации;

2) отраслевая информация специализируется по отраслям права и зако­нодательства, она может быть конституционно-правовой, административно-правовой, гражданско-правовой и т. д.;

3) международно-правовая информация, содержащаяся в международно-правовых договорах, соглашениях, конвенциях, сведения, характеризующих отно­шения между государствами, народами, международными организациями.

Ненормативная правовая информация ***это такая разновидность правовой информации, которая хотя и служит для решения задач правотворческой и правоприменительной деятельности, но не является нормативной правовой. Например, это доказательства по уголовному, гражданскому или арбитражному делу. Это может быть информация, получаемая в результате проведения судебной эксперти­зы почерка или какого-либо другого криминалистического объекта.***

Ненормативная правовая информация может быть разделена на две группы: ***информация о состоянии законности и правопорядка и информация, связанная с раскрытием и расследованием правонарушений*.**

В состав ***информации о состоянии законности и правопорядка входят*:**

1) информация о соблюдении прав и свобод человека, содержащаяся в отче­тах Уполномоченного по правам человека, в официальных данных о соблюдении Российской Федерацией своих международных обязательств, в материалах комис­сий по правам человека;

2) информация о состоянии законности и правопорядка, эффективности прокурорского надзора, содержащаяся в публикациях средств массовой информа­ции, в периодических изданиях правоохранительных и правоприменительных ор­ганов, информация о формах и способах защиты прав граждан, о принятых мерах по восстановлению законности.

В состав ***информации, связанной с раскрытием и расследованием правона­рушений*,** входят:

- криминологическая информация – данные о преступности и других право­нарушениях, эффективности уголовных наказаний;

- криминалистическая информация – информация, используемая при дока­зательстве факта преступления и идентификации лица или группы лиц, совершив­ших преступление;

- судебно-экспертная информация – информация, используемая при прове­дении судебных экспертиз для доказательства (или опровержения) факта преступ­ления и вины обвиняемого;

- оперативно-розыскная информация – информация, содержащая сведения, отражающая ход и результаты проведения оперативно-розыскных мероприятий по установлению и розыску лиц, совершивших уголовно наказуемые деяния и скры­вающихся от правосудия, а также иные сведения и материалы.

### *2.3. Система, информационные системы, управление системой.*

***Системой является совокупность взаимодействующих, относительно самостоятельных элементов, объединенных выполнением некоторой общей функции, несводимой к функциям её компонентов.***

Необходимо выделить следующие ***признаки системы:***

1) система представляет собой упорядоченную совокупность элементов;

2) элементы системы взаимосвязаны и взаимодействуют в рамках этой системы, являясь ее подсистемами. Каждый элемент системы, будучи подсистемой, характеризуется самостоятель­ностью, качественной обособленностью, в силу чего может рас­сматриваться, как самостоятельная система другого уровня;

3) система, как целое, выполняет определенную функцию, которая не может быть сведена к функциям каждого отдельно взятого ее элемента;

4) элементы системы (как подсистемы) могут взаимодейство­вать как в рамках определенной системы, так и с внешней средой и изменять при этом свое содержание или внутреннее строение.

Характеристика кибернетической системы будет непол­ной, если не добавить к сказанному, что она является *информаци­онной.*

Ст. 2. Закона об информации содержит определение понятия информационной системы. ***Информа­ционная система это организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использова­нием средств вычислительной техники и связи, реализующих информационные процессы.***

Характерной особенностью информационных систем является их способ­ность изменять свое состояние, т.е. значение определенных пара­метров, которые характеризуют систему в целом или отдельные её элементы.

***Перевод системы из одного состояния в другое путем воздействия на параметры её элементов, есть управление системой.***

###

### 3. Правовое регулирование в сфере информационных процессов.

### *3.1. Понятие, уровни, этапы информационных процессов.*

Информационные процессы в правовой системе – это про­цессы сбора, производства, распространения, преобразования, поиска, получения, передачи и потребления информации.

Информационные процессы протекают на следующих уровнях:

- общества в целом;

- больших социальных групп и социальных общностей;

- малых социальных групп и трудовых коллективов;

- отдельной личности и ее индивидуального сознания (инфор­мационно-психологические процессы).

Конституция РФ делит информационный процесс на пять этапов: поиск, получение, передача, производство и распространение информации (ч. 4 ст. 29). Схожие формулировки имеются и в других нормативных актах. В ст. 1 Закона об информации содержится более подробная формулировка – создание, сбор, обра­ботка, накопление, хранение, поиск, распространение и предоставление потреби­телю документированной информации.

В информационном процессе информация движется от источника информа­ции к ее потребителю (пользователю).

### *3.3. Юридическая природа законодательства об информации и информатизации.*

Процесс информатизации России основывается на нормах ряда отраслей российского права (конституционного, гражданского, уголовного, администра­тивного, трудового и некоторых иных). Вместе с тем общественные отношения, возникающие в процессе информатизации, не охватываются в полной мере ука­занными отраслями права. Поэтому необходимо создание и применение специального зако­нодательства об информации и информатизации. В России это новая, разви­вающаяся отрасль законодательства, регламентирует следующие вопросы:

- право гражданина и других субъектов права на различную информацию;

- правовой режим информации и информационных ресурсов;

- государственная политика и управление в сфере информатизации;

- правовое положение информационных центров, компьютерных и телеком­муникационных систем;

- информационные отношения в условиях рынка и предпринимательской дея­тельности;

- правовые вопросы оказания информационных услуг;

- вопросы собственности, владения и распоряжения информацией;

- индустрия информатизации и производство информационных технологий;

- международно-правовое сотрудничество.

В Конституции РФ впервые на конституционном уровне применен термин «информация» и производные от него термины и понятия (право на информацию, тайна информации, распространение инфор­мации и др.). Впервые в Конституцию РФ включено положение, объявляющее принципы и нормы международного права и международные договоры Российской Федерации составной частью ее правовой системы.

Подчеркивая фундаментальный характер права на информацию, Конституция РФ включила это право в число основных прав и свобод человека и гражданина. В соответствии со ст. 2 Конституции РФ право на информацию входит в категорию «высшие ценности», поскольку её режим подчиняется всему конституционному механизму, установ­ленному в гл. 1, 2 Конституции РФ.

Система источников законодательства об информации и инфор­матизации включает:

- нормы и принципы конституционного уровня; модельные и рекомендательные акты руководящих органов СНГ; международно-правовые нормы и принципы;

- федеральные законы по вопросам информатизации, специаль­ные (тематические) законы, регулирующие информационные отно­шения в отдельных сферах и направлениях общественного развития;

- указы и распоряжения Президента РФ, постановления Прави­тельства РФ, ведомственные акты, законодательство субъектов Фе­дерации, акты уголовного, гражданского, административного законо­дательства Российской Федерации, предусматривающие ответствен­ность за правонарушения в работе с документированной информацией.

Законодательство об информации и информатизации не образует в настоящее время целостной системы. Плохо разработаны теорети­ческие основы данной сферы правового регулирования. Не достаточно актов высшей юридической силы – законов. Не в полной мере используется потенциал Конституции РФ, а также зарубежный опыт.

Еще одной важной проблемой является формирование на­учных представлений об объекте информационного законодательства. Это законодательство имеет свой самостоятельный объект правового регулирования. Таким объектом являются информационные отно­шения.

***Информационно-правовое отношение*** это такое урегулиро­ванное правом отношение, при котором один субъект (физическое или юридическое лицо) вправе требовать от другого субъекта полу­чения определенной информации, а второй – обязан передать пер­вому определенный вид информации.

***Объектом*** информационных отношений выступают информация и информационные ресурсы.

***Субъектами*** информационных отношений являются общественные и государственные структуры, физические и юридические лица, пред­приятия, фирмы, объединения граждан и государство в целом.

Информационные отношения регулируются на основе информа­ционно-правовых норм.

***Информационно-правовые нормы*** это раз­новидность правовых норм, которые регламентируют права, обязанности, ответственность субъектов права при производстве, распространении и использовании информации с учетом специфики информационных отношений.

Информационные нормы можно классифицировать:

- на конституционные информационные нормы (нормы общего содержания) регламентирующие право человека на информацию, как фундаментальное право, его гарантии и механизм реализации;

- по сфере действия – универсальные, региональные, партикуляр­ные;

- по юридической силе – императивные и диспозитивные,

- по функциям в системе – материальные и процессуальные;

- по способу создания и форме существования – договорные, меж­дународные нормы, решения международных организаций.

### *3.4. Отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства.*

1. Законодательство об интеллектуальной собственности.

***А) законодательство об авторском праве и о смежных правах:***

- Закон РФ «Об авторском праве и смежных правах»;

- Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных»;

- Закон РФ «О правовой охране топологий интегральных микросхем».

***Б) Патентное законодательство:***

- «Патентный закон РФ».

***В) Законодательство о правовом режиме информации:***

- Закон РФ «О государственной тайне»;

2. Законодательство о средствах массовой информации.

- Закон «О средствах массовой информации»;

- Федеральный закон «О рекламе».

3. Законодательство о формировании информационных ресурсов, подготовке информационных продуктов, предоставлении информационных услуг.

***А) Общие вопросы законодательства об информационных ресурсах:***

- Федеральный закон «Об информации, информатизации и защите ин­формации»;

- Федеральный закон «Об обязательном экземпляре документов.

***Б) Законодательство о правовой информации:***

- Федеральный закон «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального собрания»;

***В) Законодательство о библиотечном деле:***

- Федеральный закон «О библиотечном деле»;

- Закон Краснодарского края «О библиотечном деле в Краснодарском крае».

***Г) Законодательство о международном обмене информацией:***

- Федеральный закон «Об участии в международном информационном обмене».

4. Законодательство о создании и применении информационных систем, их сетей, информационных технологий и средств их обеспечения:

- Федеральный закон «О связи».

5. Законодательство об информационной безопасности:

- Федеральный закон «О безопасности»;

### *3.5. Отдельные информационно-правовые нормы в составе нормативно-правовых актов отраслей законодательства РФ.*

***Первая группа*** – так называемые статутные акты, то есть акты, регламентирующие статус соответствующих структур. Это Конституция РФ, а также федеральные конституционные законы и федеральные законы, устанавливающие статус органов государственной власти, как на федеральном уровне, так и на уровне субъектов Федерации, статус общественных объединении.

***Вторую группу*** составляют акты гражданского законодательства, прежде всего Гражданский кодекс РФ.

***В третью группу*** входят законодательные акты, регулирующие от­ношения в различных отраслях хозяйственной деятельности, в част­ности законодательство о земле, о недрах, об охране природы и т.д.

***К четвертой группе*** относятся акты об ответственности за правона­рушения в информационной сфере, прежде всего, Уголовный кодекс РФ и Кодекс РСФСР об административных правонарушениях.

### 4. Подготовка правовой информации к машинной обработке.

### *4.1. Понятие и способы формализации правовой информации.*

***Формализа­ция это выявление и уточ­нение содержания изучаемого явления через рассмотрение и фиксацию его формы и оперирование с ней.***

Принципы построения и использования формализационной системы описания:

Любая формализационная система должна располагать таким набором средств описания, которые позволяли бы описать не только общие, но и частные признаки, как количественные, так и качественные характеристики объекта познания;

2) Универсальность т.е. пригодность к использованию задач хотя бы одного класса;

3) Должна строится на базе содержательного описания. При осуществлении формализации необходимо участие не только юриста, но и прикладного математика, т.к. юрист не сможет дать логичной и четкой математической формулировке стоящей задаче.

Метод формализации используется при вводе правовой информации в па­мять ЭВМ. Информация предварительно должна быть представлена в формаль­ном виде и закодирована.

Средствами формализации правовой информации являются:

- математические методы;

- символы и стандартизованные обозначения;

- методы логики, в частности математической логики;

- специальные коды (кодирование криминальной информации);

- социальное измерение;

- статистические методы.

Процесс формализации информации тесно связан с *абстрагированием* – логическим приёмом выделения главных, наиболее существенных при решении данной зада­чи признаков, после чего выделенные признаки формализуются.

### *4.2. Сущность и виды метризации правовой информации.*

В широком плане под ***метризацией*** понимается описание какого-либо объекта определенной совокупностью числовых характеристик.

Различают два ***вида метризации:***

- ***подсчет*** – при подсчете в ка­честве средства выражения интересующих данных ис­пользуют натуральные числа;

- ***измерение*** – при измерениях в качестве средства выражения полу­ченных данных наряду с натуральным числом используют­ся принятые для каждого вида измерений соответствующие единицы меры.

***Объектами измерения*** могут выступать любые предме­ты и явления материального мира, обладающие определен­ными свойствами, которые могут выражаться в большей или меньшей степени и, следовательно, могут быть оценены количественно.

Данные, которые получаются в результате измерения, называются ***параметрической (измерительной) информацией*.**

Итак, под ***метризацией правовой информации следует понимать такую процедуру ее обработки, в результа­те которой субъект юридической деятельности получает ко­личественные характеристики тех или иных параметров объекта познания.***

В метрологии измерения подразделяют на три основных вида: ***прямые, косвенные и совокупные (совместные).***

Получаемые с помощью приведенных выше видов из­мерений количественные характеристики могут иметь дво­якое выражение:

- в тех случаях, когда мы можем непосредственно изме­рить определенное свойство объекта (например, его длину, вес), полученные результаты именуют ***абсолютной количе­ственной характеристикой;***

**- *относи­тельная количественная характеристика*** есть выражение отношения соответствующих абсолютных характеристик одна через другую.

***Необходимость и значимость*** их использования опреде­ляются рядом факторов.

1) В ряде случаев существует ситуация, когда механизм формирования информации, содержащей­ся в том или ином источнике, нам не известен и мы не зна­ем способа его определения. Например, на исследование по­ступили два или несколько фотопортретов, запечатлевших лицо человека в разных ракурсах и изготовленных при не­известных нам условиях (неизвестны примененная оптика, положение лица в кадре, дистанция съемки и т. п.).

2) В отдельных источниках информации абсо­лютные ее характеристики в количественном отношении могут варьировать в весьма значительном диапазоне, тогда как относительные характеристики более устойчивы.

Характерным примером в этом отношении является по­черк, у одного и того же лица одни и те же письмен­ные знаки или их элементы могут иметь разные размеры как в одной и той же, так и в разных рукописях. В то же вре­мя такая характеристика, как соотношение абсолютных раз­меров одинаковых знаков или их элементов, может оста­ваться постоянной или варьироваться крайне незначительно.

3) Встречаются случаи, когда абсолютные харак­теристики получить вообще нельзя либо весьма затрудни­тельно по техническим причинам. Чаще всего это имеет ме­сто при использовании физических методов исследования, в частности, такого, как метод эмиссионного спектрального анализа.

### *4.3. Кодирование правовой информации.*

В широком смысле под ***кодированием понимаются опе­рации замены каких-либо данных (например, текстовых) сокращенными условными обозначениями, как правило, цифровыми или символами.*** Обратная операция называется ***декодированием****.*

Обычно эти операции используются как средство представления информации, характеризующее индивидуальные особенности объекта или исследуемого события, в виде по­следовательно расположенных символов абстрактного алфа­вита, комбинацию таких символов называют *кодом*.

Кодовые символы могут иметь различную форму. Чаще всего это цифры, буквы какого-либо алфавита, а также раз­личного рода условные знаки и их сочетания (точка и тире, математические символы и т. п.).

***Требования предъявляемые к способам кодирования правовой информации*:**

1) способ кодирования должен обеспечивать применимость избранных исследователем средств и мето­дов анализа познаваемого объекта и способствовать опти­мизации решения поставленной задачи;

2) получаемый с его помощью информацион­ный аналог объекта исследования должен содержать данные, однозначно и достаточно полно (для решаемой задачи) ха­рактеризующие индивидуальные особенности объекта-ори­гинала;

3) он должен позволять преобразовывать (когда это необходимо) получаемый код в другой вид, а от последнего возвращаться к исходному;

4) он должен обеспечивать получение макси­мально емкого сообщения, которое вместе с тем было бы достаточно содержательно и удобно для его практического использования.

В настоящее время используются различные ***способы кодирования правовой информа­ции*.**

1) ***Простые координатные сетки, точечное и контурное ко­дирование, при этом*** автоматизация самого процесса кодирования обычно отсутствует.

Достоинство кодирования с помощью координатной сетки состоит в том, что формализованное описание объек­та исследования можно дать в виде числового ряда, состоящего из единиц и нолей. Это очень удобно, поскольку позволяет использовать сигнал любой физической природы для переноса информации на расстояние и ввести ее в память машины или построить та­кой объект на приемном устройстве получателя информа­ции.

Недостатком этого способа является то, что практически невоз­можно однозначно передать характер объекта при его слож­ной конфигурации (например, все особенности начертания букв в исследуемом тексте).

2) ***Точечно-зональное кодирование контура*** слагается из следующих операций:

- введение объекта, предварительно нормированного по размеру, в систему координат в соответствии с правилами, учитывающими характер непосредственного объекта исследования и применяемой методики;

- квантование объекта исследования – процесс преобразования каких-либо величин с непрерывной шкалой значений в величину с прерывной (дискретной) шкалой. Особое значение имеет выбор места наложения кодировочных точек;

- заключительный этап: считывание количественных характеристик. Особенно широко этот приём метризации и кодирования используется в судебной экспертизе (дактилоскопия, почерковедение и др.) и автоматизированных информационно-поисковых системах.

Все известные ныне *методы кодирования информации* по степени автоматизации подразделяются на три вида:

***ручное*** (выведение дактилоскопической формулы);

***полуавтоматическое*** (ранние версии АДИС «ПАПИЛОН», «СОНДА-ФРЕС» и т.д.);

***автоматического кодирова­ния***(поздние версии АДИС «ПАПИЛОН», «СОНДА-ПЛЮС» и т.д.).

### 5. Автоматизированные системы правовой информации.

# *5.1. Общие вопросы автоматизированных систем.*

***Банком данных*** (БД) называется совокупность спе­циальным образом организованных данных (программ­ных, технических, языковых и методических средств), предназначенных для обеспечения, накопления и исполь­зования этих данных.

***База данных*** это совокупность взаимосвязанных дан­ных, организованная по определенным правилам. Базой данных являются специальным образом организованные один либо группа файлов. Для работы с ними использу­ется система управления базой данных. При этом под­разумевается, что база данных определена по схеме, не зависящей от программ, которые к ней обращаются.

В соответствии со ст. 1 Федерального закона «О правовой охране программ для ЭВМ и баз данных» от 23 сентября 1992 г. «*база данных* это объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизирован­ных таким образом, чтобы эти данные могли быть най­дены и обработаны с помощью ЭВМ».

База данных предназначена для хранения больших массивов информации, быстрого поиска нужных сведе­ний и документов. Она создается в любой информацион­ной системе.

Большой эффект дает создание информационных баз, ориентированных на специальные виды правотвор­ческой деятельности. Так, база информационного обес­печения законопроектной деятельности в сфере инфор­мации и информатизации включает:

- координационные планы разработки нормативных правовых актов в сфере информации и информатиза­ции;

- специальные нормативные акты всех уровней по проблемам законодательства в сфере информации и информатизации;

- акты, в той или иной мере связанные с информа­цией и информатизацией;

- проекты нормативных актов, разрабатываемые в сфере информации и информатизации;

- акты зарубежного законодательства;

- информация о ведущих ученых и специалистах в сфере информатизации, разработчиков проектов нор­мативных правовых актов;

- терминология, используемая в проектах норматив­ных правовых актов;

- публикации в средствах массовой информации;

- литература по законодательству в сфере инфор­мации и информатизации.

***Системой управления базами данных*** (СУБД) на­зывается комплекс программных средств, предназначен­ных для создания банка данных, поддержания данных в состоянии, пригодном для использова­ния, организации доступа пользователей в усло­виях принятой технологии обработки данных.

В организации систем правовой информации важное место принадлежит по­нятию «файл». ***Файл*** это наименьшая область памяти компьютера, выделенная для хранения части массива данных, набор записей, обладающих некоторыми струк­турными элементами и семантическими признаками. К организации файлов относят; логические формулиров­ки данных, т. е. содержание записей, которые входят в файл; группировку данных в физические записи, т. е. блокирование и сегментацию записей; порядок следо­вания записей и их элементов.

### *5.2. Автоматизированные информационно поисковые системы (АИПС).*

***Автоматизированная информационно-поисковая система (АИПС) это система информационных, мате­матических, программных, лингвистических, организа­ционных и технических средств, предназначенная для накопления и коллективного использования норматив­ной правовой информации.***

АИПС состоит из четырех основных элементов:

1) документального и поискового массива;

2) информацион­но-поискового языка, правил индексирования и критерия выдачи информации;

3) электронно-вычислительных, технических, математи­ческих и программных средств;

4) людей, эксплуатирующих систему.

Создание АИПС правовой информации опирается на решение следующих ***задач:***

- определение качественных и количественных ха­рактеристик правовой информации;

- разработка наиболее эффективных способов сбора и распространения правовой информации;

- определение критерия отбора источников инфор­мации для введения в поисковую систему;

- разработка информационных алгоритмов;

- набор процедур автоматизированного поиска нор­мативно-правовых актов в памяти ЭВМ с большим объе­мом информации;

- проведение социологических исследований деятель­ности различных государственных учреждений, ведомств и организаций в целях выявления тенденций, опреде­ляющих развитие правовой информационной практики.

В основе АИПС правовой информации находятся базы и банки информации.

***Информационный запрос*** представляет собой вопрос або­нента о законодательстве на определенную правовую темати­ку в форме консультации.

Совокупность ключевых слов из текста документа, пере­веденных в форму информационно-поискового языка, со­ставляет его ***поисковый образ,*** который вводится в ЭВМ для формирования ее информационной базы.

Совокупность ключевых слов из текста запроса абонента, преобразованных в форму информационно-поискового язы­ка, составляет его ***поисковое предписание,*** которое вводится в ЭВМ для проведения и реализации информационного по­иска.

***Информационный тематический поиск*** в АИПС являет­ся пословным (побуквенным), т. е. основан на правиле срав­нения символов заиндексированного документа с символа­ми заиндексированной темы запроса. Если та или иная ком­бинация символов, составляющих поисковое предписание запроса, отыскивает в памяти ЭВМ точно такую же схему знаков, формирующих поисковый образ документа, то нуж­ная информация найдена. Иными словами, пословный (побуквенный) поиск означает, что для его реализации лексические элементы (термины или словосочетания), составляющие поисковое предписание запроса, должны быть сформулированы точно в таком же виде, как в поисковых образах документов на соответствующую тему, ранее введенных в ЭВМ.

При такой процедуре важное значение имеет выделение в документе тех терминов, смысловое значение которых отражает его основное содержание, и их использование при информационном поиске.

Слова или словосочетания в форме информационно-поискового языка содержатся в тезаурусе (информационно-поисковом словаре).

Таким образом, чтобы заиндексировать тексты правового документа и за­проса, следует отобранные из них ключевые слова перевести в форму инфор­мационно-поискового языка, т. е. составить поисковый образ документа и по­исковое предписание запроса. Как уже отмечалось, поисковое предписание вводится в ЭВМ для формирования ее информационной базы, а поисковое предписание запроса – с целью реализации поиска информации.

***Автоматизированный информационный поиск*** это процедура извлечения необходимых або­ненту сведений из хранящегося в ЭВМ документального массива с помощью использования в этих целях логико-се­мантических, электронно-вычислительных, технических, программных, математических средств общения человека с компьютером.

Автоматизированный информационный поиск в самом общем виде можно подразделить на два вида:

***1) поиск по основным реквизитам нормативного акта*** (названию, номеру, виду акта, органу, принявшему акт, дате принятия акта); использование этого вида поиска не вызывает практических трудности, когда абоненту известны один или несколько реквизитов интересующего его правового документа. Если же абонент знает название, или номер, или дату принятия акта, то для успешного осуществления информационного поиска достаточно и одного из перечисленных реквизитов;

***2) тематический по­иск,*** в большинстве случаев абонент не располагает никакими сведениями об адресах нужной ему информации. Абоненту необходимы документы, регулирующие тот или иной вопрос, то или иное правоотношение. При этом ему неизвестно ни количество принятых по соответствующему вопросу нормативных актов, ни их номера, ни названия и т. д. В таких ситуациях проводится поиск информации по ее тематическому содержанию.

Методы компьютерного поиска правовой информации необходимо совершенствовать. Одна из возможностей данного направления – создание гипертекстовых баз знаний.

***Гипертекст*** это особая форма организации и пред­ставления текстового материала.

Большинство текстов любой природы, включая и правовые, содержат наряду с основным также и неко­торые иные тексты – второго порядка.

Примерами текстов второго порядка являются: си­стема ссылок к тексту, комментарии к нему, его раз­ные редакции, тексты, отвечающие или возражающие друг другу и др.

Гипертекстовые технологии содержат правила пе­рехода от одного текста к другому с использованием ЭВМ.

### *5.3. Автоматизированные информационно-логические системы (АИЛС).*

Перспективным направлением развития общей и правовой информатики является применение новейших компью­терных технологий, к которым относятся интеллектуальные системы и техноло­гии, базирующиеся на идеологии искусственного интеллекта.

***Искусственный интеллект*** это искусственно созданная система, реализуе­мая на современных ЭВМ и предназначенная для моделирования свойств реального интеллекта человека, его мыслительной деятельности, психики, т. е. способности выбора и формирования целесообразного решения на основе ра­нее имеющейся информации.

Применение интеллектуальных систем и технологий в области права вклю­чает следующие направления:

- интеллектуализация автоматизированных информационно-поисковых си­стем (АИПС) по законодательству;

- создание автоматизированных систем анализа нормативных правовых тек­стов;

- создание консультационных систем по правотворчеству;

- создание экспертных систем в сфере правоприменительной деятельности;

- разработка алгоритмов и программ идентификации при помощи ЭВМ в расследовании и рассмотрении судебных дел (сфера криминалистики и судебной экспертизы).

### *5.4. Автоматизированные системы управления (АСУ).*

***Автоматизированные системы управления (АСУ) это человеко-машинные системы управления, основанные на применении электрон­но-вычислительной техники, экономико-математических методов и на взаимодействии в процессе управления челове­ка и ЭВМ, на функциональном разделении труда между ни­ми.***

При этом на ЭВМ возлагаются функции получения, хранения, анализа, переработки информации. За человеком, остаются наиболее сложные процессы использования инфор­мации для постановки проблем, определения целей, приня­тия решений, а также контроль за работой ЭВМ.

***Основная цель*** автоматизации организации управ­ления состоит в обеспечении оптимального управления и оптимального функционирования объекта управления, что означает правильный выбор целей и средств их достижения, а также наилучшем определении задач и распреде­ление заданий между частями системы, осуществление вза­имодействия всех частей.

***Первый вид АСУ*** – автоматизирована только обработка информации, и АСУ способна лишь достоверно отображать состояние управляемых объектов. С ее помощью решаются справочные задачи, а также учетные и расчетные задачи.

***Второй вид АСУ*** отличается тем, что система может вы­ступать в роли про­гнозиста*,* т.е. на основе анализа информации может создавать несколько различных вариантов проектов решений и представлять их человеку для выбора.

***Третий вид АСУ*** – система действительно выступает, как управляющая в полном смысле слова: выдает управленче­ские решения или управляющее воздействие в иной форме (команда, сигнал, текст документа, и др.), которое исполняет­ся управляемой системой.

Существующие виды АСУ нередко дополняются автома­тизированной функцией контроля за исполнением приня­тых решений.

### *5.5. Автоматизированные обучающие системы (АОС).*

***Автоматизированные обучающие системы (АОС) это программно-технические комплексы, обеспечи­вающие накопление, систематизацию и предъявление зна­ний, контроль усвоения знаний, выбор оптимальной стратегии обучения и форми­рование у обучаемых необходимых умений и навыков.***

К числу автоматизированных обучающих систем относятся экспертно-обучающие системы и экспертно-моделирующие обучающие системы.

***Экспертно-обучающие*** системы обеспечивают ряд прин­ципиально новых возможностей, главной из которых явля­ется способность ответа на запрос пользователя, сформули­рованный в терминах предметной области, способность производить ло­гические выводы и обобщения.

***Экспертно-моделирующие*** обучающие системы оказыва­ют пользователям помощь в процессе анализа проблемной ситуации и поиска рационального решения задачи на основе имитационных моделей.

Различные направления автоматизированного обучения могут быть классифицированы в зависимости от специфики управляющих воздействий системы обучения на обучаемого и способов организации учебного материала.

В связи с этим выделяются следующие ***методы автоматизированного обу­чения:***

программирование учебной деятельности;

моделирование учебной среды;

свободное обучение;

тестирование;

информирование.

Указанные методы конкретизируются в типах автомати­зированного обучения.

Выделяются следующие ***типы автоматизированного обучения:***

- программно-управляемое обучение;

- автоматизированная проверка знаний;

- автоматизированное тренирование.

### 6. Компьютеризация правотворческой и правоприменительной деятельности.

### *6.1. Компьютеризация правотворческой деятельности.*

***Под компьютеризацией правотворчества понимается внедрение в эту сферу государственной деятельности новейших информационных технологий и экспертных консультативных систем, создание крупных информационных центров. Её перспективное направление – приме­нение интеллектуальных систем и технологий на базе идей искусст­венного интеллекта, как главного направления информатики и вы­числительной техники.***

Правотворческий процесс является информационным и представ­ляет собой сбор и обработку информации. В нем первичная юриди­ческая, экономическая, политическая, социальная и иная необходимая для подготовки нормативно-правового акта информация преобразуется в правовую – в нормы и институты права, в юридические формулы и правила поведения различных субъектов права.

Создание правовых норм является мыслительным, твор­ческим процессом и остается исключительным приорите­том человеческой деятельности. О применении в правотворчестве ЭВМ можно говорить в смысле ор­ганизационно-подготовительной, вспомогательной работы. Иначе говоря, ЭВМ в данном случае является механизмом информационного обеспечения для непосредственно право­творческой деятельности.

Аналитическо-правовая работа в условиях колоссаль­ного массива правовой информации и традиционных форм ее организации (т. е. вручную) чрезвычайно трудоемка и требует длительного времени, поэтому ***компьютеризация правотворческой деятельности объективна.***

На Парламентскую библиотеку, Парламентский Центр, издательство Федерального Собрания и др. структуры возложено информационное обеспечение Федерального Собрания и Государственной Думы. Результативным средством улучшения качества этой де­ятельности является применение современных быстродействующих ЭВМ.

Практике известны различные ***формы использования ЭВМ в правотворческом процессе*:**

- создание автоматизированных инфор­мационно-поисковых систем по законодательству;

- компьютерное моделирование объема юридических понятий;

- электронное голосование, автоматизированный анализ нормативно-правовых текстов;

- система­тизация и хранение нормативных актов.

Вместе с тем практика выдвигает новые формы применения ЭВМ в законопроектной деятельности. К их числу относится *компьютерный мониторинг* – процедура динамики законодательного про­цесса.

В Главном правовом управлении при Президенте Российской Фе­дерации создана система компьютерного мониторинга ***«Ведение за­конопроекта»*.** В базе системы находятся: исходный вариант законо­проекта, промежуточные варианты, вплоть до окончательного, этапы движения законопроекта во всех государственных органах; сведения о лицах, ответственных за состояние законопроекта, а также о лицах и органах, давших на него заключение; поступившие от заинтересованных и должностных лиц предложения.

Система позволяет получать сведения о результатах обсуждения законопроекта в Государственной Думе, Совете Федерации, о под­писании его Президентом РФ и об опубликовании принятого закона.

В Аппарате Государственной Думы создана и фун­кционирует ***электронная база нормативно-правовой ин­формации «Закон»*.** Объем базы – свыше 70 тыс. доку­ментов федеральных органов государственной власти и органов субъектов Федерации. Ежегодно число доку­ментов, хранящихся в компьютере, возрастает на не­сколько тысяч. В нормативные акты посто­янно вносятся изменения и дополнения в соответствии с действующим законодательством.

В ходе подготовки и проведения избирательных кампаний на всех уровнях собирается и обрабатывается значительное количество информации. Для этого создана и функционирует Государственная автомати­зированная система (ГАС) «Выборы» – общероссийская система, функциони­рующая на принципах совместимости и взаимодействия с фе­деральными и региональными системами и сетями в рамках единого информационного пространства Российской Федера­ции и предназначенная для информационного обеспечения хода избирательных кампаний всех уровней.

### *6.2. Компьютеризации правоприменительной деятельности.*

***Применение права*** это государственно-властная деятельность компетентных органов, состоящая в специально организованных дей­ствиях (актах), при реализации юридических норм по отношению к конкретному случаю.

***Основным субъектом*** правоприменительной деятельности является суд, он осуществляет ее путем отправления правосудия. Органы прокуратуры и МВД реализуют ее в рамках своей компетенции. Эта же деятельность осуществляется органами исполнительной власти, а также должностными лицами всех уров­ней при выполнении ими своих обязанностей.

Данная деятельность связана с особым видом информационной деятельности – юридическим доказыванием. Это деятельность субъектов права, направленная на установление с по­мощью юридических доказательств истинных обстоятельств дела. Про­цесс юридического доказывания опирается на особый вид информа­ции – юридические доказательства.

***Объективной необходимостью внедрения ЭВМ в правоприменительную деятельность явилось то, что имеющаяся у правоприменительных органов информация достигла таких размеров, что не могла уже обрабатываться вручную, потребовалась её автоматизация с помощью компьютеров.***

Виды автоматизированных систем используемых в правоприменительной деятельности.

В целях информационного обеспечения правоприменительной дея­тельности во всех правоприменительных и правоохранительных ор­ганах создаются глобальные информационные системы. Такие системы создаются в Конституционном Суде РФ, Верховном Суде РФ, Выс­шем Арбитражном Суде РФ, в системе органов прокуратуры, Ми­нистерстве юстиции РФ, Министерстве внутренних дел РФ.

В базах данных этих систем сосредотачивается значительная ненор­мативная информация, соответствующая профилю деятельности каж­дого органа.

Общая концепция компьютеризации правоприменительной деятель­ности претерпела существенные изменения. В 70-е годы процесс создания автоматизированных систем в юри­дической сфере находился под влиянием концепций, свя­занных с созданием АСУ (автоматизированных систем управления). В результате этого стали создаваться АСУ-МВД, АСУ-Прокуратура, АСУ-Юстиция, АСУ-Вер­ховный Суд.

На рубеже 70-80-х годов концепция информатизации правоприменительных органов значительно изменилась. В системе юридических учреждений нет управления в собственном смысле слова, речь идет об отправлении правосудия, борьбе с преступностью, осуществлении прокурорского надзора и тому подоб­ных сферах собственно юридической деятельности. Поэтому из прак­тических разработок стал исчезать термин «АСУ». На смену пришли другие понятия: АСИО-Прокуратура, АСИО-Юстиция, специализированная территориально распределенная автоматизированная сеть МВД (СТРАС-СК), что является значительно более точным и правильным.

### *6.3. Получение информации для правотворческой и правоприменительной деятельности.*

В настоящее время информацию для правотворческой и правоприменительной деятельности можно получить.

1. В информационно-вычислительных сетях МВД РФ (ГИЦ МВД РФ).

2. В системе информационного обеспечения органов и учреждений юстиции.

В рамках данной системы создана и функциониру­ет подсистема статистической информации. Система предназначена для сбора и обработки дан­ных о деятельности судов, а также учреждений и орга­нов юстиции (количество рассмотренных судебных дел – уголовных и гражданских и т. п.).

3. В автоматизированной системе информационного обеспечения органов прокуратуры.

4. Из компьютерных центров и сетей.

***4.1. Научно-технический центр «Система.*** В соответствии с Указом Президента РФ «О мерах по реализации правовой инфор­матизации России» от 28 июня 1993 г. на научно-техни­ческий центр правовой информации «Система» возложены функции голов­ного органа в сфере правовой информатизации. В за­дачи этого центра входит формирование эталонного банка данных правовой информации и создание цент­рального узла системы правовой информации.

Научно-техническим центром «Система» формиру­ются еженедельные электронные бюллетени «Собрания законодательства Российской Федерации». Информационно-поисковая система «Свод законов Российской Им­перии» в машиночитаемом виде содержит 16 книг официального издания «Свода законов Российской Им­перии».

***4.2. Автоматизированная система информационного обеспечения органов и учреждений юстиции*** разрабатывается Министерством юстиции РФ, в рамках которого создано и функциони­рует специальное Управление правовой информатиза­ции. Система призвана решать задачу информационно­го обеспечения деятельности органов и учреждений, входящих в Министерство юстиции РФ.

Система снабжает правовой информацией все ра­боты по подготовке проектов нормативных правовых актов, которые поступают в аппарат Министерства юстиции РФ и обес­печивает правотворческую деятельность ряда высших органов власти – Государственной Думы, Совета Фе­дерации, а также Главного правового управления Пре­зидента РФ.

Центральным звеном системы является Научный центр правовой информации при Министерстве юсти­ции РФ (НЦПИ). НЦПИ предоставляет информацию пользователям СНГ, Совета Европы и ООН. Одновременно он является главным методическим цен­тром научных исследований в сфере правовой инфор­матики. Все программы Центра функционируют в со­ставе аппаратно-программного комплекса «Фонд».

Архив НЦПИ насчитывает более 70 000 докумен­тов, в числе которых нормативные акты бывшего СССР. В соответствии с постановлением Правительства Рос­сийской Федерации от 21 октября 1994 г. № 1181 НЦПИ осуществляет сбор, учет и распространение нормативных актов министерств и ведомств Российской Федера­ции.

Созданная в Центре база «Эталон» представляет собой базу данных с действующими официальными редакциями текстов нормативных актов. Тексты законодательных нормативных актов имеют ссылки на их официальное опубликование, а тексты ведомственных нормативных актов – ссылки на регис­трацию в Министерстве юстиции РФ.

База данных «Эталон» содержит:

- действующие нормативные акты бывшего СССР (с 1992 г.);

- нормативные акты высших представительных и законодательных органов РФ, Президента и Правитель­ства РФ, принятые начиная с 1990 г., а также все ра­нее принятые, в которые внесены изменения;

- общеобязательные нормативные акты министерств и ведомств, прошедшие регистрацию в Министерстве юстиции РФ;

- нормативные акты межгосударственного характе­ра СНГ;

- правовые акты Мэрии и Правительства г. Москвы.

***4.3. Получение информации от негосударственных организаций.*** В необходимых случаях правотворческие и правоприменительные органы могут получать нормативную правовую информацию и от негосударственных организаций (компьютерных фирм).

Среди негосударственных (частных) компьютерных фирм лидирующее положение занимает Научно-производ­ственное объединение «Гарант» (созданное в 1990 г.).

По заказу Государственной Думы НПП «Гарант-Сервис» разрабатывает компьютерные средства для законотворческой и законопроектной деятельности. Пра­вовое управление Государственной Думы успешно применяет компьютерные базы марки «Гарант»: «Тол­ковый словарь нормативных определений» и «Алфавитно-предметный указатель к Гражданскому кодексу». Кро­ме того, разработан шестиязычный словарь бизнеса и права.

Другая компьютерная фирма – Акционерное объе­динение «Консультант-Плюс», объединяет 300 региональных информационных центров, произво­дящих поставку справочных правовых систем, сервис­ное обслуживание и передачу информации пользовате­лям.

Технология «Консультант Плюс» позволяет обнов­лять информационный банк пользователя без его пол­ной замены, требующей больших материальных и вре­менных затрат.

Одним из приоритетных направлений работы «Консультант Плюс» является сотрудничество с правоохранительными органами.

***4.4. Из международных сетей,*** т.е. совокупности компьютеров, образующих системы передачи и обработки данных. Ком­поненты сети расположены в нескольких странах.

В сеть Интернет представили свою информацию практически все научные организации США, в том чис­ле Корнельский институт юридической информации США; школа права Университета штата Индиана, юри­дические ресурсы Колумбийского университета, архив школы права Сиднейского университета, а также за­конодательство информационно развитых стран.

Мировой компьютерной сетью является и сеть Ин­терпола. Она охватывает полицейские органы и учреж­дения 177 стран, имеет своей целью информационное обеспечение оперативной работы полицейских органов всего мира и работы по раскрытию и расследованию преступлений. Компьютерная сеть Интерпола является весьма эффективным средством борьбы с международ­ной преступностью.

Конгрессом США разработан проект Всемирной ком­пьютерной сети правовой информации. Она призвана объединить и сделать доступными массивы норматив­ных актов всех государств.

### 7. Использование INTERNET в профессиональной деятельности юриста.

### *7.1. Глобальная сеть Интернет – связь, информация.*

Крупнейшей всемирной компьютерной сетью является сеть Интернет. Она выросла из сети «Арпанет», созданной четверть века назад для обмена информа­цией между рядом исследовательских центров военной промышленности США. Интернет дает возможность общения и передачи информации между любыми компьютерами по всему миру вне зависимости от того, какие это компьютеры, т.е. решена большая проблема – проблема совместимости (поскольку общаются компьютеры самых разных типов, операционные системы в которых значительно отличаются друг от друга).

К сети «Интернет» подсоединены все парламенты Западной Европы. Подсоединены юридические органы и учреждения России – Президент, Правительство, Государственная Дума, Совет Федераций, Конституционный Суд, Верховный Суд, Высший Арбитражный Суд, Министерство юстиции и т.д. Информация, которая может в таких случаях использоваться, представляет собой данные, юридические документы храня­щиеся в центрах юридической информации, в библиотеках парламентов других стран.

***Связь.***Без сомнения, основной инструмент из богатого арсенала Интернета, который прежде всего использу­ется юристом, – система электронной почты. Не вдаваясь в технические подробности этой техно­логии, просто отметим, что электронная почта позво­ляет быстро и дешево передавать любые массивы ин­формации от одного пользователя Интернета к другому.

***Информация.*** В стороне от почты стоит другая составляющая часть Интернета – система Word Wide Web (WWW, «все­мирная паутина») – наиболее быстрорастущая часть Сети. WWW, по сути, является удобным и понятным способом представления информации. Любые данные размещаются на экране компьютера в виде наглядных статей и картинок.

### *7.2. Поиск правовой информации.*

Основной метод поиска информации в Интерне­те – обращение к специальным бесплатным поиско­вым серверам.

Поисковый сервер это специализированный компьютер (их часто называют «поисковые машины»), который непрерывно автоматически исследует ресур­сы Сети. Обращаясь на такой сервер со своим персональным запросом, пользователь получает ответ. Например, если вы зададите определенный термин (наберете с клавиатуры интересующее вас слово или словосочетание в специальном окне), сер­вер выдаст перечень всех страниц, на которых он когда-либо встречал такое слово.

Предпочтение следует отдавать тем поисковым серверам, которые производят поиск по наибольшему количеству адресов, позволяют форму­лировать сложные запросы, а также уже имеют гото­вые каталоги ресурсов по различным темам.

Рекомендуются следующие поиско­вые серверы:

**Рэмблер** – *www. rambler. ru.*

Содержит миллионы документов с более чем 15000 сайтов. Имеет развитый язык за­просов и гибкую форму вывода результатов. Есть простой поиск и расширенный (кнопка «advanced»). При расширенном поиске вы указываете, где искать слово (в целом по российским серверам, по россий­ским конференциям, в именах (в адресах www...ru), в названиях документов, в заголовках документов, в на­чале документов), период, за который производить поиск, исключения (слова, при наличии которых до­кумент не указывается в ответе).

Большой интерес на Рэмблере представляет каталог ресурсов.

**Яндекс** – *www. yandex. ru.*

Поиск в нем ведется по 11300 серверам (более 2,5 миллиона документов). Чтобы задать запрос, надо написать в строке запроса то, что вам нужно (например, защита прав потребителя в строке запроса и вы получите список адресов документов, в которых встречаются все эти слова в разных падежах и числах. А если вы хотите получить только те документы, где эти слова стоят подряд, используйте кавычки – «защита прав потребителя».

Полезной оказывается и функция поиска в уже готовом списке. Например, вы получили результат по первому запросу. Теперь вы можете еще более кон­кретизировать свои требования: выберите «искать найденном» и введите дополнительное слово, например, «неустойка». Список результатов еще более сузится.

**Апорт** – *www. aport.ru.*

Уступая в количестве документов вышеописанным конкурентам, он очень удобен. Прежде всего – формой представления результатов поиска. Выдастся достаточно точная информация о документе, его дата, степень соответствия запроса в процентах, краткие выдержки из текста документа, содержащего слова запроса.

Задавая запрос, вы также можете воспользоваться некоторыми дополнительными функциями: автоматически исправить ошибки в запросе, заказать перевод запроса с русского на английский или, наоборот таким же образом заказать перевод результата.

**Yahoo** – *www.yahoo.com.*

Это самый популярный поисковый сервер в мире. Ежедневно к его услугам прибегает более 2,5 миллиона человек. Yahoo, безус­ловно, – механизм для поиска в зарубежном Интернете.

Yahoo не русифицирован, но за­просы на русском языке подавать можно, и при этом большинство ответов будут вполне читаемыми. Гло­бальный размах сервера позволяет иногда найти дей­ствительно важную и редкую правовую информацию.

**AltaVista** – *www.altavista.digital.com.*

Если Yahoo служит базовым поисковым механиз­мом, то AltaVista следует использовать для расширен­ного поиска – в целом он выдает большее количество результатов и в расширенной форме. Привлека­тельная возможность сервера – поиск информации на строго определенном языке, в том числе и на русском.

Существует большое количество и других зарубежных поисковых серверов.

### *7.3. Российские правовые ресурсы Сети.*

Правовые новости. Интернет имеет достаточно неплохие правовые «электронные газеты».

На странице агентства «Экономика и жизнь» *www.akdi.ru/akdi.htm,* можно прочитать свежие и полезные статьи по праву. Интерес представляют рубри­ки: «Арбитражная хроника», «Комментарии к измене­ниям в экономическом законодательстве», «Человек и государство» и другие.

По адресу *ms.park.ru/monitoring* вы найдете еще одну разновидность юридической информации – регулярно обновляемые мониторинги нормативных актов. Мони­торинг – это краткое описание нормативных актов с изложением их основной мысли, сути вносимых изме­нений, возможно – предыстории издания.

На указанной странице комментарии к новым нор­мативным актам появляются ежедневно.

Несколько иначе выглядят короткие мониторинги со страницы московской фирмы «Клевер» *(www.moscow.klever. net/labas/topnews.html).* Они обновляются не ежедневно, в результате мониторинг выглядит, как большая статья, разбитая на главы по отраслям права. Но, пожа­луй, самое важное достоинство «клеверовских» мониторингов состоит в том, что к каждому комментарию при­лагается сам текст комментируемого акта.

Юридические услуги. В Сети имеются полноценные серверы юридических организаций.

Сервер Московской городской коллегии адвокатов «Арбитражсудправо» *(www.advokat,ru.).* Данный сервер отличает одна интересная особен­ность: адвокаты предусмотрели возможность для кли­ента связаться с ними напрямую через Интернет, используя электронные средст­ва Сети, можно установить голосовую связь (по интернет-телефону) или текстовый диалог (чат), опера­тивно отправить короткое сообщение.

Особый интерес в последнее время вызывает воз­можность юридического консультирования через Ин­тернет. Вот один из способов виртуальной консульта­ции: на странице *park.ms.ru/consult* размещен обшир­ный тематический каталог вопросов-ответов по праву, построенный по отраслевому принципу. Если в числе имеющихся ответов вы решения своей пробле­мы не найдете, вам будет предложено задать назрев­ший вопрос консультантам сервера (ответ – по элек­тронной почте).

Электронные конференции по праву. Одна из наиболее популярных форм общения в Интернете – электронные конференции. Они могут проходить в виде переписки, когда все желающие ос­тавляют на определенной странице свои мнения либо в прямом эфире.

Открыта правовая телеконференция «Налоговая система России» *www. garant. ru/win/project*.

По адресу *www.garant.ru/win/project1*проводится обсуждение юридической проблемы – права на доступ к информации.

Примером интерактивной (в прямом эфире) кон­ференции по праву является семинар на тему «Право и Интернет» *(www.vic.spb.ru/seminar/seminar.htm).* За­тронутая тема – взаимодействие права и Сети «Ин­тернет» – является в настоящее время одной из наи­более актуальных и в то же самое время малоизучен­ных.

Безо всяких препятствий вы можете принять учас­тие в любой из перечисленных конференций и лиш­ний раз испытать свое юридическое мастерство и профессиональное умение спорить.

### *7.4. Правовая телеконференция «Налоговая система России».*

По адресу http: // www. garant. ru/win/project/ открыта правовая телеконференция «Налоговая система России», в рамках которой существуют три раздела.

1. В разделе «Основы налоговой системы России» предлагается обсуждение любых правовых проблем уплаты налогов. Главной темой являются коллизии, имеющие несколько путей решения и интересные как с точки зрения их практического разрешения, так и с позиций теории правовой науки. Посетитель может предложить участникам конференции для обсуждения какую-либо проблему или ознакомиться с мнениями других юристов.

2. В разделе «Налоговая реформа» имеются комментарии и аналитические материалы по Налоговому кодексу РФ. Как и в предыдущем разделе, посетители имеют возможность свободно вести правовые споры по проблемам налоговой реформы.

3. В раздел «Проблемы правоприменительной практики» помещены ответы на самые сложные юридические вопросы налогообложения, выработанные в результате дискуссий. Данный раздел дает юристам шанс не совершать ошибок, работая с налоговым законодательством.

### *7.5. Сайт Верховного Суда России.*

Сайт это один или несколько адресов Интернета, на которых лицо или организация предоставляет информацию, которая часто включает в себя переходы к другим местам, где нужная информация может быть найдена.

В декабре 1997 г. во всемирной компьютер­ной сети «Интернет» был открыт официальный сер­вер Верховного Суда Российской Федерации *(www. supcourt.ru).* На данном этапе он является одним из наиболее информа­тивных и полезных правовых ресурсов Сети.

Большое количество пользователей при­влекает информация, касающаяся дея­тельности Суда: законодательство о судеб­ной системе Российской Федерации, сборники доку­ментов и решений Суда, расписание рассмотрения дел в коллегиях, справочная информация.

Раздел «О Верховном Суде РФ» содержит полный список должностных лиц Суда с указанием рабочих телефонов (руководство, должностные лица всех от­делов и управлений), списки членов судебных колле­гий; на Председателя и его заместителей имеются неболь­шие личные досье с фотографиями. В раздел также включена информация о распорядке личного приема судьями граждан с жалобами в порядке надзора и выдержки из Инструкции по делопроизводству Вер­ховного Суда РФ от 18 ноября 1996 г., касающиеся личного приема.

Раздел сервера «Бюллетень Верховного Суда» включает в себя полные электронные версии «Бюлле­теня Верховного Суда» начиная с № 1 за 1997 год.

Участник рассматриваемого в Верховном Суде дела, может найти полезные для себя сведения в разделе «О назначении дел к разби­рательству в судебных коллегиях». Здесь «вывешива­ется» график рассмотрения дел по всем трем коллеги­ям, их инстанциям и судебным составам на ближай­шую неделю.

Следующий раздел сервера – «Решения 1-й ин­станции Гражданской коллегии Верховного Суда РФ». Он имеет подразделы: Президент РФ, Государственная Дума, Министерство государст­венного имущества, Государственная налоговая служ­ба, Министерство внутренних дел, Министерство экономики, Министерство здравоохранения. В этот блок должны включаться все решения коллегии за последние два года в виде кратких сводок.

Раздел сервера «Совет судей» задуман как источ­ник оперативной профессиональной информации для соответствующих должностных лиц, однако пока он еще в процессе формирования. Сейчас здесь можно посмотреть некоторые документы, касающиеся су­дейского сообщества.

В раздел «Судебный департамент» включен новый федеральный закон «О Судебном департаменте при Верховном Суде Российской Федерации» № 8-ФЗ от 8 января 1998 г.

Наконец, раздел официального сервера Верховного Суда РФ «Последние новости». Здесь есть подборка последних указов Президента о назначении судей, а также подраздел «Хроника меж­дународных связей Верховного Суда».

### *7.6. Словари по юриспруденции.*

Для корректного перевода с иностранного языка в Интернете, компанией «Гарант» разработана технология созда­ния электронных словарей по юриспруденции. На данный момент в этой технологии реализованы три вида словарей – мультиязычный словарь серии *«Бизнес и право»*, словарь де­финиций *«Нормативные определения»* и многоязычный словарь *«Eurovoc»*.

Для работы с нормативными актами на иностранных язы­ках был разработан шестиязычный словарь *«Бизнес и право»*. При работе с ним пользователь может ввести искомое слово и получить его написание на любом из поддерживаемых языков – русском, английском, французском, немецком, испанском или итальянском. В словарь включено около 13 тыс. слов и словосочетаний, такой большой словарный запас гарантирует нахождение практически любого необходимого термина. С помощью данного словаря легко решается широкий круг задач, связанных с переводом, тол­кованием и применением юридических текстов.

Словарь «Бизнес и право», не ограничиваются простым переводом. Словарь содержит подробные определения приводимых в нем терминов на русском и английском языках, являясь одновременно и межъязыковым, и толковым.

Толковый словарь законодательных дефиниций *«Норма­тивные определения»* – совместная разработка компании «Гарант» и Правового управления Аппарата Государственной Думы. Словарь содержит более 2 тыс. определений терминов, закрепленных в законодательстве в качестве нормативных.

Многоязычный словарь *«Eurovoc»* – система, которая используется уже более 10 лет для индексирования и поиска данных в информационно-поисковых системах официальных документов органов, учреждений, институтов Европейского Союза и ряда государств – членов ЕС. Основной целью его адаптации и перевода на русский язык является обеспечение пользователям доступа к многоязычному информационно-поисковому средству, признанному в качестве международного терминологического стандарта. Составление русской версии словаря было осуществлено парламентской библиотекой. Компания «Гарант» в рамках проекта «Инфор­мационные технологии для законотворчества» реализовала русскую версию *«Eurovoc»* в своей программной оболочке. «Eurovoc» включает в себя более 6400 терминов, каждый из которых представлен на русском, английском и французском языках.

Словарь предназначен в первую очередь для специалис­тов, принимающих участие в процессе законотворчества либо занимающихся аналитической деятельностью. С помощью «Eurovoc» становится возможным обеспечить стандартизацию используемых терминов и единый подход к обработке документов.

### 8. Общеюридические информационные системы.

*8.1. Российская автоматизированная система информации о нормативно правовых актах (РАСИНА).*

Российская автоматизированная система информации о норматив­ных правовых актах – одна из важнейших государст­венных систем, которая будет обеспечивать информацией о норматив­ных правовых актах (НПА) всех возможных пользователей. Она отражает структуру органов государственной власти, в кото­рой каждый из этих органов формирует эталонный банк принимаемых им актов, обновляет их в связи с текущим правотворчеством и пред­ставляет копии этих банков в специальный центр, обеспечивающий доведение информации об актах до широкого круга потребителей пра­вовой информации.

РАСИНА строится как динамическая система, представляемая сетью распределенных эталонных банков НПА органов государствен­ной власти, интегрального эталонного банка НПА этих органов в Рос­сийском центре правовой информации (РосЦПИ), эталонных банков в региональных центрах правовой информации (РЦПИ) субъектов фе­дерации и на территориях. В соответствии с решением Правительства РФ эталонные банки общеобязательных НПА министерств и ведомств РФ (банки ведомственных НПА) ведет Научный центр правовой ин­формации (НЦПИ) Министерства юстиции РФ.

При разработке РАСИНА используются принципы:

- активного участия государственных структур в создании и исполь­зовании информационно-правовых ресурсов РФ;

- децентрализованного формирования и актуализации эталонных банков НПА органов, их принимающих, и совместного использования копий эталонных банков при информационно-правовом обеспечении;

- отработки типовых проектных решений в опорных зонах с последу­ющим внедрением по всем территориям и регионам России;

- использования имеющихся программных, технических средств, средств связи и передачи информации с целью экономии ресурсов на создание систем;

- совмещения возможностей централизованного и децентрализован­ного информационно-правового обслуживания в зависимости от коли­чества запросов, поступающих в единицу времени, и скоростных воз­можностей существующих каналов передачи информации.

### *8.2. Справочно-правовые системы семейства «Консультант-Плюс.*

Семейство «Консультант Плюс» состоит из комплекса следующих систем: справочные правовые системы «Консультант-Плюс»: Версия Проф.; «Консультант-Плюс»: Эксперт Приложение; «Консультант-Плюс»: Россия – СНГ; «Консультант-Плюс»: Московский и Санкт-Пе­тербургский выпуски, а также справочных систем «Консультант-Бухгал­тер», «Консультант-Плюс»: Арбитраж, «Деловые Бумаги», «Ценные Бу­маги». Структура комплекса определена характером документов, содер­жащихся в каждой из частей, и позволяет эффективно организовать работу с колоссальным объемом информации.

Документы включаются в ту или иную часть информационного комплекса после юридической обработки (исследования взаимосвязи между документами и формирования ссылок, составления справочных сведений, ретроспектив различных редакций) и анализа, состоящего из определения степени их юридической значимости и влияния на эконо­мические процессы. Каждая часть комплекса построена на стандарт­ной программной технологии «Консультант-Плюс». Информацион­ный комплекс дает возможность получать как общезначимую, так и более специализированную правовую информацию.

Справочная правовая система «Консультант-Плюс» содержит все законодательные и нормативные правовые акты Российской Федера­ции, в том числе документы свыше 80 министерств и ведомств.

Новые документы еженедельно поступают в комплекс «Консуль­тант-Плюс» по прямым договорам об информационном обмене с орга­нами государственной власти Российской Федерации: Администра­цией Президента РФ; Советом Федерации; Государственной Думой; Центральным банком РФ; Министерством финансов РФ; Высшим Ар­битражным Судом РФ; Государственным антимонопольным комите­том РФ; Федеральным управлением по делам о несостоятельности; Министерством труда и социального развития РФ; Федеральным фон­дом обязательного медицинского страхования и др.

Обслуживание пользователей производится региональными информационными центрами сети «Консультант-Плюс».

Общероссийская сеть распространения правовой информации «Консультант Плюс» насчитывает более 300 региональных центров по всей территории Российской Федерации. Новая информация ежеднев­но поступает в региональные центры по сетям телекоммуникаций. Это позволяет специалистам с одинаковой эффективностью использовать комплекс «Консультант Плюс» в любой географической точке страны.

Информационные центры сети «Консультант Плюс» предоставля­ют следующие услуги:

- установку комплекса и обучение работе с ним;

- передачу новой информации в комплекс – по модемной связи или курьерской службой центра;

- поиск документов но индивидуальному заказу;

- помощь в решении технических проблем (например, перенос ком­плекса с одного компьютера на другой, восстановление комплекса при сбоях компьютера пользователя и т.п.);

- бесплатный выезд специалиста для установки демонстрационного варианта комплекса на компьютер и ознакомительной консультации.

### *8.3. Информационно-правовая система «Кодекс».*

Информационная правовая система «Кодекс» (ИПС «Кодекс») это компьютерная система, предназначенная для использования на персональных компьютерах IBM PC или в локальных компьютерных сетях. Назначение системы состоит в том, чтобы обеспечить оператив­ный доступ пользователя к электронной юридической библиотеке, размещенной в памяти компьютера, содержащей полные тексты законода­тельных и нормативных актов Российской Федерации, местных орга­нов власти, документов международного права, законодательных актов иностранных государств, тексты комментариев, образцы типовых договоров, а также другие информационные материалы, включающей более 25000 документов и материалов.

ИПС «Кодекс» разработана «Центром компьютерных разработок» (ЦКР) в г. Санкт-Петербурге, который занимается коммерческим рас­пространением и обслуживанием системы «Кодекс».

Возможности технологического сервиса «Кодекса» позволяют организовать информационное обслуживание больших групп пользова­телей как в пределах одного здания, так и территориально удаленных друг от друга.

ИПС «Кодекс» осуществляет информационное обслуживание, включающее получение новых нормативных документов и внесение всех изменений в нормативные акты, оперативное обновление баз дан­ных, установленных у пользователя. Базы данных «Кодекс» пополня­ются ежедневно, информация в базы данных поступает из официаль­ных источников – государственных органов власти и официальных изданий. Пакеты обновления баз данных передаются пользователям системы еженедельно.

### *8.4. Универсальная система поддержки правоприменения «Гарант».*

Справочная правовая система «Гарант» (СПС «Гарант») разработа­на научно-производственным предприятием (НПП) Гарант-Сервис в1990 г. «Гарант» – разработка, реализованная без использова­ния существующих систем управления базой данных (СУБД).

Ядром системы является гипертекст как технология организации системы ссылок между информационными блоками, позволяющая оп­тимальным образом проследить взаимосвязи между документами, что особенно важно при работе с нормативными актами.

Нормативные акты поступают в «Гарант» непосред­ственно из Администрации Президента РФ, Правитель­ства РФ, Министерства финансов РФ, Центрального банка РФ, Государственного таможенного комитета РФ, Государственной налоговой службы РФ, Высшего Ар­битражного Суда РФ, других официальных источников. Правовые Базы и Справочники составляют спра­вочную правовую систему «Гарант». Федеральное зако­нодательство представлено в универсальных и специа­лизированных правовых базах. Универсальная база «Законодательство России» объединяет подборки основ­ных документов по всем разделам законодательства. В системе «Гарант» представлено банковское, таможен­ное, жилищное, земельное законодательство, уголов­ное и административное право, международное право (Россия – СНГ), судебная и арбитражная практика. Рос­сийское законодательство представлено в сети Интер­нет.

По заказу Государственной Думы НПП «Гарант-Сервис» разрабатывает компьютерные средства для законотворческой и законопроектной деятельности. Пра­вовое управление Государственной Думы успешно применяет компьютерные базы марки «Гарант» - «Тол­ковый словарь нормативных определений» и «Алфавитно-предметный указатель к Гражданскому кодексу». Кро­ме того, разработан шестиязычный словарь бизнеса и права.

### *8.5. Юридическая справочно-информационная система (ЮСИС).*

Программный комплекс ЮСИС (ПК ЮСИС) функционирует в операционных средах MS-DOS и MS-WINDOWS на ПЭВМ типа IBM PC, в том числе с использованием в локальных сетях. Ежеднев­ное обновление баз данных комплекса обеспечивается включенной в него программой установления телекоммуникационной связи.

Комплекс отличается универсальностью, так как, с одной стороны, обеспечивает поиск и ввод нормативных правовых актов, в том числе ведомственных, научно-практического комментария к ним, данных су­дебной, арбитражной и нотариальной практики применения по всем отраслям права Российской Федерации, а с другой – дает возможность пользователю вести собственную базу правовой и другой необходимой информации, включая делопроизводство. Система не тре­бует от пользователя специальных знаний компьютерной техники и юриспруденции, в силу чего комплекс применяется не только юриста­ми-профессионалами.

Базы данных ПК ЮСИС обновляются ежедневно и передаются пользователям как по коммутируемым, так и по выделенным каналам.

ПК ЮСИС обслуживает одновременно две сопряженные между собой базы данных:

1) аннотированной информации (в виде картотеки) о принятых нормативных актах и практике их применения;

2) текстов нормативных актов, документов и т.д.

Программное обеспечение позволяет пользователю получать об­новление базы данных в телекоммуникационном режиме не выходя из системы.

Помимо задач, связанных с правоприменительной деятельностью пользователей, ПК ЮСИС предоставляет возможность создания ло­кальных (региональных) баз данных в его структуре и логического сопряжения документов федерального уровня с документами органов законодательной и исполнительной власти субъектов федерации и местных органов, что существенно облегчает работу пользователей.

### 9. Использование ЭВМ в организации и методике расследования.

### *9.1. Общая характеристика использование ЭВМ в организации и методике расследования.*

Компьютерные технологии получают всё большее распространение в расследовании.

Сотрудниками органов внутренних дел затрачивается до 25-30 % служебного времени на заполнение всевозможных справок, отчётов и других материалов. Потребность органов внутренних дел в необходимой информации удовлетворяется примерно на 30-35 %, а в оперативно-розыскной лишь на 20-25 %[[6]](#footnote-6).

В организации использования информационных технологий в расследовании существует ряд проблем.

Основными направлениями внедрения ЭВМ в расследование являются компьютеризация – организации и методики расследования преступлений, автоматизации криминалистических учётов, а также судебных экспертиз. Эти направления и являются основными. Существуют и другие направления. Например, обучающие системы по организации и методике расследования. Наконец, компьютер используется просто, как средство оргтехники при подготовке различных справок, текстов заключений экспертов и т.д.

В использовании компьютерной техники в расследовании можно выделить такие вопросы, как определение направления использования; основные объекты применения и методы использования ЭВМ внутри каждого направления (производство экспертиз криминалистические учёты и др.); рациональное применение имеющейся техники в различных правоохранительных органах (следственный отдел, уголовный розыск и т.д.); активное взаимодействие в системе человек-машина.

Важнейшим направлением использования компьютерной техники является компьютеризация организации и методики расследования преступлений.

Организация расследования есть его упорядочение, создание мысленной модели предстоящей деятельности[[7]](#footnote-7). Как известно, организация расследования складывается из формирования целей, определения предмета расследования и конкретизации предмета доказывания, планирования, создания условий для оптимального производства следственных и иных действий и т.д. В последние годы личный состав следственных подразделений постоянно меняется, не все следователи обладают достаточной базой знаний. Даже опытные следователи при проведении сложных и особо сложных расследований могут допустить упущения. Поэтому даже им, не говоря о молодых и неопытных, требуется обращаться к научным рекомендациям. Однако поиск, пользование ими затруднительно, отсюда вытекает необходимость их обобщения, сжатия, автоматизация поиска нужной части определённой рекомендации и т.д. Для этой цели информацию необходимо закодировать, создать компьютерную программу.

Теоретической основой создания программ расследования является положение о том, что элементы предмета доказывания: место, время, обстановка, условия совершения преступления и другие, при всей их индивидуальности поддаются типизации[[8]](#footnote-8).

На данным момент созданы и применяются методики, содержащие статистический анализ следственных ситуаций, охватывая указанные элементы.

Если можно типизировать элементы предмета доказывания то подлежат типизации и следственные ситуации, а также появляется возможность введения в компьютер данных о типичных доказательствах.

Следовательно, появляется возможность формирования массива данных для типовых программ расследования. Такая программа должна включать в себя криминалистическую (разрабатывается криминалистом), которая включает в себя элементы структуры расследования и кибернетическую (создаётся программистом исходя из криминалистической) части.

Автоматизация организации и методики расследования преступлений идёт двумя путями: справочно-информационное обеспечение и решение логико-поисковых задач. В настоящее время первое направление преобладает.

Справочно-информационные системы позволяют следователю быстро в любое время иметь информацию, касающуюся расследуемого события и процесса расследования.

В последнее время создаются системы, выполняющие логические операции, в которых некоторые функции за следователя осуществляет машина.

Действующие системы, как было сказано, основаны на научно-практических рекомендациях. В перспективе разрабатываются системы по организации и методике расследования преступлений, включающих в себя также и опыт расследования определённой категории дел[[9]](#footnote-9). Такие предложения были и раньше. Так Н.А. Селиванов предпринял попытку обобщить для последующей кодировки данные по делам об убийствах, опубликованных в сборниках «Следственная практика».

Создание такой системы имело бы большое положительное значение для практических работников, которые «получили бы практическое обоснование для принятия решения в виде опыта аналогичного расследования»[[10]](#footnote-10).

Однако, создание такой системы наталкивается на определённые трудности в кодификации необходимой информации, вероятно в ближайшем будущем эта система всё же будет создана.

В управлении расследованием, существуют автоматизированные системы управления (АСУ), автоматизированные системы информационного обеспечения (АСИО), специализированная территориально распределенная автоматизированная сеть Следственного комитета МВД РФ (СТРАС-СК). И хотя они ещё далеки от совершенства, системы такого уровня позволят осуществлять контроль за сроками и законностью материалов нижестоящего звена правоохранительных органов. Обмен информацией в них предполагается осуществлять с помощью модемов и коммутирующих соединений по обычным и специальным телефонным линиям. На наш взгляд, эти системы должны быть полностью совместимы между собой для обмена информацией, и представлять собой единый банк данных общефедерального уровня. Проблема здесь заключается в финансировании, отсутствия необходимых средств в бюджете. В США давно функционируют системы такого уровня.

Другим направлением являются обучающие системы по организации и методике расследования.

Автоматизация организации и методики расследования преступлений идёт двумя путями: справочно-информационное обеспечение и решение логико-поисковых задач. В настоящее время первое направление преобладает.

Справочно-информационные системы позволяют следователю быстро в любое время иметь информацию, касающуюся расследуемого события и процесса расследования.

В последнее время создаются системы, выполняющие логические операции, в которых некоторые функции за следователя осуществляет машина.

Указанные системы основаны на научно-практических рекомендациях.

### *9.2. Управление системой расследования.*

Для управления системой расследования созданы и хорошо зарекомендовали себя автоматизированные системы – ***АСИО Прокуратура и СТРАС-СК*** *МВД*, хотя они ещё далеки от совершенства.

Для информационного обеспечения прокуратуры создана автоматизированная система инфор­мационного обеспечения – ***АСИО - Прокуратура.***

С помощью данной системы реализуются 4 задачи:

- зако­нодательство – обеспечивает правовыми актами всех ра­ботников прокуратуры, в том числе следователей, пу­тем использования консультационных систем различ­ного вида;

- жалоба предназначена для регистрации заявлений и жа­лоб граждан, в том числе по уголовным делам;

- стати­стика;

- кадры.

Органы прокуратуры имеют три уровня: Генеральная прокуратура РФ; прокуратуры краев, об­ластей, республик и иные, приравненные к ним; и горрайпрокуратуры.

1. В Генеральной прокуратуре имеются локальные вычислительные сети в соот­ветствии с перечисленными задачами.

2. Для краевых, областных прокуратур помимо сис­тем, функционирующих в городских и райпрокуратурах, необходимы АСИО, обусловленные характером этого второго уровня организации и управления рас­следованием:

- АСИО обработки информации по уголовным делам с продленными сроками или содержания обви­няемых под стражей (Сроки),

- АСИО по уголовным делам о преступлениях, совершенных организованными группами (Органи­зованная преступность).

3. Для городских и районных прокуратур внедряются следующие АИС:

- Автоматизированная система информационного обеспечения надзора за исполнением законов при про­изводстве предварительного следствия и дознания.

- Автоматизированная система информационного обеспечения надзора за рассмотрением заявлений и сообщений о совершенных преступлениях (Регистрация).

- АСИО надзора за обоснованностью отказов в возбуждении уголовных дел.

- АСИО обработки сведений по надзору за след­ствием и дознанием, за законностью судебных поста­новлений по уголовным делам.

- АСИО расследования преступлений:

а) о массовых беспорядках на межнациональной основе;

б) о нарушении правил безопасности движения на железнодорожном транспорте;

в) о нарушении правил безопасности движения на морском транспорте;

г) об умышленных убийствах, совершенных:

- на сексуальной почве;

- сопряженных с разбойным нападением на жилища;

- с целью завладения автомототранспортом и др.

В МВД России осуществляется разработка сис­темы ***СТРАС-СК*,** со специализированными банками данных. Информационное обеспечение этой системы включает три уровня:

- для центрального аппарата Следственного комитета МВД РФ;

- для следственных управлений (отделов) МВД-УВД;

- для следственных подразделений горрайорганов внут­ренних дел.

Информационное обеспечение СТРАС-СК разрабатывает­ся в виде ряда подсистем, формируемых по следующим ма­гистральным направлениям:

1. ***Подсистема «Расследование»*,** предназначена для поддержки следователя при принятии решений в процессе расследования уголовного дела. Данная подсистема строится на основе элементов частных криминалистических методик расследования отдельных видов преступлений (криминалистических характеристик, типичных следственных ситуаций, типовых следственных версий). Функционирова­ние системы осуществляется в виде АРМ (автоматизирован­ного рабочего места) следователя.

2. ***Подсистема «Контроль»*** используется для автоматизации учетно-контрольной и вспомогательной деятельности следователя, на­копления и использования информации о делах, находя­щихся в производстве и на контроле.

3. ***Подсистема «Статистика»*** предназначена для автоматизации формирова­ния и анализа статистических данных, осуществляет на­копление данных о преступлениях и использование этих данных в целях получения информации статистического характера и др.

4. ***Справочная подсистема правовой и методической ин­формации*** по действующему законодательству Российской Федерации, Постановлениям Пленума Верховного Суда РФ, ведомственным нормативным актам МВД, МЮ, Прокура­туры и других ведомств, затрагивающих деятельность следст­венных подразделений.

5. ***Подсистема федеральных, централизованных и региональных банков данных***по уголовным делам некоторых категорий (хищени­ям денежных средств по подложным авизо, фальшивомонет­ничеству и другим).

6. ***Подсистема связи*** с Федеральным банком криминальной информации ГИЦ МВД РФ и региональных банков криминальной информации ИЦ МВД, ГУВД, УВД для получения информации из оперативно-справочных и криминалистичес­ких учетов.

7. ***Вспомогательные подсистемы*** для автоматизации работы секретариатов, канцелярии и учета кадров следственных ап­паратов.

Обмен информацией между указанными системами предполагается осуществлять с помощью модемов и коммутирующих соединений по обычным и специальным телефонным линиям. Эти системы должны быть полностью совместимы между собой для обмена информацией, и представлять собой единый банк данных общефедерального уровня.

В управлении системой расследования как в про­куратуре, так и в МВД компьютеризация направлена на достижение следующих основных целей:

- сбор, концентрация сведений о расследуемых уголовных делах; автоматизация контроля за соблюде­нием процессуальных сроков при расследовании уго­ловных дел;

- автоматизация контроля за рассмотрением жа­лоб и заявлений участников процесса и граждан по расследуемым уголовным делам;

- создание и использование баз данных передо­вой следственной и судебной практики и научно-практических рекомендаций по расследованию престу­плений, информационно-поисковых систем (АИПС) по расследованию отдельных видов преступлений;

- информация об обеспечении расследования специалистами: в ходе следственных действий и про­изводстве экспертиз – экспертных учреждениях, видах экспертиз;

- анализ информации о нераскрытых преступлениях, рекомендации по их раскрытию;

- анализ работы по предупреждению преступле­ний;

- составление управленческих документов;

- анализ статистической отчетности.

### *9.3. Компьютеризация иных элементов расследования.*

Для проведения оператив­ной и учетно-аналитической работы в органах МВД РФ применяются следующие АИСС (автоматизированные информационные сис­темы связей):

***«Сводка»*** - позволяет работать с базой данных, создаваемых по поступающей в ОВД опера­тивной информации о происшествиях и преступлениях, осущест­влять поиск в БД по реквизитам, а также вести статистическую обработку данных, составлять отчеты при поступлении запросов и после исполнения документов;

***АИСС «Гастролёры»*** - предназначена для автоматизиро­ванной обработки оперативными подразделениями УВДТ и ОВДТ информации о лицах, представляющих оперативный инте­рес для органов внутренних дел на транспорте, и их связях; о похищенных на транспорте, неразысканных или добровольно сданных вещах, имеющих индивидуальные номера или характер­ные особенности;

***АИСС «Грузы-ЖД»*** - разработана для автоматизированного сбора, хранения и выдачи информации о фактах хищения груза и багажа на железнодорожном транспорте, по которым возбуждены уголовные дела, а также о раскрытых хищениях грузов;

***АИСС «Наркобизнес»*** - предназначена для сотрудников отдела по незаконному обороту наркотиков. Использование сис­темы позволяет выявлять лица, их связи с событиями, друг с другом, оружием и адресами, проходящими по разным видам учетов;

***АИСС «Картотека-Регион»*** - предназначена для работы с пофамильными учетами осужденных, разыскиваемых и задер­жанных за бродяжничество лиц;

***АИСС «Спецаппарат»*** - предназначена для работы со спецаппаратом и позволяет планировать оперативно-розыскные мероприятия на основе быстрого и качественного обеспечения их необходимой информации. Можно, например, быстро найти круг лиц, проходящих по однотипным фактам из массива спецсооб­щений, способам совершения преступлений, адресам и т.п.[[11]](#footnote-11)

### *9.4. Обучающие системы по организации и методике расследования.*

Составляющей информационных техноло­гий являются программное обеспечение учебного процесса, это, по существу, особый класс программ –обучающие системы. Данные системы все время совершенствуют­ся, появляются новые версии. Среди автоматизированных обучающих систем наиболее распространены: контрольно-обучающие, консультационные поисковые системы, экспертно-моделирующие.

**1. Контрольно-обучающие системы** представляют собой различные программы-тесты, их разра­ботка в настоящее время облегчается наличием универсаль­ного программного обеспечения в виде «оболочек», по­зволяющих по единой схеме разрабатывать программы для самых различных юридических дисциплин. Наполнение «оболочек» материалами для учебных занятий не требует знания программирования.

Прохождение обучаемым программы может быть услож­нено и дифференцировано за счет ограничения времени на ответ, за счет дифференциации предъявляемых для выбора альтернатив по степени их правильности и точности, за счет замены вопроса конкретной проблемной ситуацией, что приближает теоретическое обучение к практическому.

Контрольно-обучающие программы на основе ЭВМ вполне могут быть использованы в процессе проведения экзаменов и зачетов, что может значительно повысить объ­ективность оценки знаний и резко сократить затраты време­ни на данный вид учебной работы.

**2. Консультационные поисковые системы**: Гарант, Консультант-Плюс, Кодекс используются как практическими юристами, так и для обучения студентов навыкам поиска правовых документов.

Положительным фактором применения данных систем является то, что студентами приобретаются навыки поиска документов по всем отраслям права.

**3. Экспертно-моделирующие системы по криминалистике** или как они ещё называются **ККДИ** (компьютерные криминалистические деловые игры), позволяют во время практических занятий, криминалистических учений, во время самостоятельной работы студентов имитировать следственную ситуацию, требующую от обучаемых приня­тия процессуальных и тактических решений. Используются они и для подготовки и самоподготовки следователей

Рассмотрим используемые компьютерные деловые игры: «Следователь», «Убийство», «Рэкет», «Мираж», «Расследование изнасилова­ний».

***ККДИ «Следователь»*** пред­назначена для практического обучения по темам, связанным с методикой расследования краж, грабежей, разбоев, угонов автот­ранспорта, совершаемых устойчивой преступной группой наркоманов.

Работу по данной программе можно начинать по любой из десяти вводных – исходных данных о совершении различных преступлений. По итогам работы обуча­емые должны выйти на установление всех участников группы и всех эпизодов совершения преступления, несмотря на то, с какой вводной они начали работу.

Игра завершается принятием решения о привлечении винов­ных лиц в качестве обвиняемых по различным эпизодам преступ­ной деятельности.

ККДИ «Убийство» предна­значена для формирования умений и навыков расследования такой распространенной категории преступлений, как бытовые убийства. Особенностью данной игры является моделирование ситуаций, когда следователю приходится оценивать всю совокупность со­бранных им доказательств для принятия таких решений, как задержание подозреваемых, привлечение в качестве обвиняемых, избрание меры пресечения в виде содержания под стражей. При этом возможны процессуальные ошибки следователя, на которые система адекватно реагирует в обучении.

Данная ККДИ может быть использована при изучении методи­ки расследования преступлений несовершеннолетних, а также некоторых разделов уголовного процесса, связанных с привлече­нием в качестве обвиняемых и применением принудительных мер в процессе расследования.

ККДИ «Рэкет» предусматривает принятие всего комплекса основных процессу­альных решений и ориентирована на формирование умений и навыков расследования дел, совершенных организованными груп­пами. Исходная информация связана с заявлением потерпевшей о факте квалифицированного вымогательства. В процессе расследования обучаемые должны изобличить членов преступного формирования в совершении вымогательства и выйти на иные эпизоды преступной деятельности (иные вымога­тельства, разбойное нападение).

В данной системе особое внимание уделено отработке умения и навыков выявления не только исполнителей тех или иных пре­ступлений, но и установления других членов преступных группи­ровок (организатора, наводчика, укрывателя). Особое внимание уделено проблемам взаимодействия следователей с оперативны­ми работниками подразделений по борьбе с организованной пре­ступностью и коррупцией. Данная система позволяет отрабаты­вать вопросы, связанные с использованием новых возможностей раскрытия преступлений и доказывания вины, в частности с использованием результатов прослушивания телефонных перего­воров.

***ККДИ «Мираж»*** может быть использована при практической отработке учебных вопросов, связанных с комплексным использованием сил и средств при раскрытии тяжких преступлений. Здесь перед обучаемыми возникает задача выявления членов преступной группы и их изобличения. В данной ККДИ больше внимания уделено вопросам оперативно-розыскной деятельности.

***ККДИ «Расследование изнасилований»*** предназначена для формирования навыков рассле­дования половых преступлений, связанных с назначени­ем экспертизы. Большое внимание уделено вопросам реагирования на поступающие заявления, сообщения о преступле­ниях; установления неизвестного лица, совершившего преступле­ние. В данной системе предусмотрены возможности количествен­ной оценки результатов работы обучаемых.

### 10. Автоматизация криминалистических учетов.

### *10.1. Общая характеристика автоматизации криминалистических учетов.*

Следующим не менее важным направлением является автоматизация криминалистических учётов.

Первые попытки внедрения ЭВМ в юридическую деятельность были предприняты в первую очередь в области автоматизации криминалистических учётов и в частности дактилоскопических.

Автоматизация преследует многие цели, основными из которых являются: оперативность (короткий промежуток времени между запросом и получением результата), возможность выяснения преступлений совершённых одним лицом на определённой территории и т.д.

Различают криминалистические учеты банки данных о событиях, явлениях криминального ха­рактера, их отдельных элементах, в том числе людях.

Объекты криминалистического учета разнообраз­ны: отпечатки пальцев, живые лица, трупы, стреляные пули, гильзы и др. Сами эти объекты или их описания для использования в АИПС подвергаются определен­ной обработки. Она заключается в описании объектов в избранных (определенных для данной системы) тер­минах, т.е. объекты формализуются. Совокупность та­ких формализованных описаний и составляет банк данных системы.

Криминалистические учеты сосредоточены в МВД России и осуществляются в двух больших подразделе­ниях этого ведомства. Собственно уголовная регистра­ция сосредоточена в Главном информационном центре МВД РФ и информационных центрах в регионах. Опе­ративно-розыскная информация накапливается также в экспертно-криминалистических подразделениях; управ­лениях, отделах, отделениях, группах. Возглавляет эту систему экспертно-криминалистический центр МВД РФ.

Большой объем информации, содержащейся в централизованных (федеральных) и местных криминалистических учетах, широкий круг пользователей обу­словил создание автоматизированных информационных систем.

Оптимальное информационное обеспечение рас­следования должно включать:

- создание интегрированных банков данных;

- обмен информацией между системами;

- передачу документации, текстов, изображений, речи, сообщений;

- информационную службу сети;

- обеспечение пользователям, в том числе следо­вателю, оперативному работнику, непосредственного доступа к информации, хранящейся в различных бан­ках данных.

Банки данных включают федеральные, региональные банки данных горрайорганов внут­ренних дел. В перспективе желательно подключение пользователей к банкам данных «Государственного комитета по наркотикам и незаконному обороту наркотических средств» и иных органов расследования. Речь идёт об использовании информации на всех уровнях правоохранительной деятельности, интеграции систем в информационно-вычислительные сети отраслевого и регионального уровней, обеспечение их взаимодействия с системами различных ведомств.

К банкам данных прямой доступ должны иметь, как сотрудники низовых звеньев информационной службы, так и следователи.

### *10.2. Автоматизированные дактилоскопические идентификационные системы и сходные с ними по принципу работы системы.*

Определенные трудности возникли в проверке по следотекам и дактилокартотекам, ведущимся в экспертно-криминалистических подразделениях органов внутренних дел, следов пальцев рук, изымаемых с мест нераскрытых преступлений и дактилокарт лиц, представляющих оперативный интерес. С ростом преступности возросли и массивы следотек и картотек. Качественная проверка, по ним стала невозможной. Поэтому остро встала проблема оснащения экспертно-криминалистических подразделений ОВД автоматизированными дактилоскопическими идентификационными системами. Существовавшие зарубежные системы (например, «ПРИТРАК», «МОРФО» и др.) имели высокую цену, у них не было адаптации к российской специфике. Требовалось более высокое качество изымаемых следов и дактилокарт.

 Необходимо отметить, что функционирующие в настоящее время в США различные компьютерные системы используют принципы, сформулированные ещё в начале 50-х российским криминалистом Л. Эджубовым, однако американские разработчики никогда не упоминают этого [[12]](#footnote-12).

Активно работы по созданию отечественных АДИС (автоматизированных дактилоскопических идентификационных систем) начались в 1989 г. Была изучена возможность автоматизации распознания отпечатков пальцев с помощью персональных компьютеров, разработаны алгоритмы, программы фильтрации и сжатия изображений, автоматического индексирования отпечатков пальцев, проведены исследования методов идентификации изображений отпечатков. В 1992 году созданы отечественные АДИС. С 1993 года Экспертно-криминалистическим центром МВД РФ проводится эксперимент по внедрению АДИС в органах внутренних дел. В базовых экспертно-криминалистических подразделениях МВД России размещены для опытной эксплуатации АДИС «СОНДА-ФРЕС» («СОНДА-ПЛЮС»), «ПАПИЛОН», «ПО­ИСК», «ДАКТО-ПРО», «АРМЭК» и др.

 На современном этапе в России наиболее эффективной признана АДИС «ПАПИЛОН», которая функционирует в ГУВД Краснодарского края.

Автоматизированные дактилоскопические идентификационные системы осуществляют следующие функции:

1) Ввод изображений и дактилокарт в память компьютера;

2) Обработка и индексирование (копирование) дактилоскопических изображений. Обозначаются признаки узора папилярных линий (в среднем 15 - 17 признаков).

3) Хранение введенной информации в базе данных.

4) Поиск в базе данных по запросной информации и выдача рекомендательных списков поисковых образов.

При вводе в базу данных новых дактилокарт выполняется поиск по всем ранее введенным отпечаткам и массиву следов, обновляются рекомендательные списки (поиски «карта – карты» и «карта – следы»).

Аналогичные проверки выполняются при вводе каждого нового следа (поиски «след – отпечатки» и «след – следы»). Оператору предоставляется возможность сравнить на экране монитора изображение запросного следа и отпечатков из рекомендательного списка с выделением отдельных фрагментов в увеличенном масштабе. Специальный указатель отмечает точки следа и отпечатка, признанные системой схожими.

Рекомендательный список позволяет визуально установить степень соответствия следа отпечатку. При желании оператор может детально исследовать на экране монитора фрагменты изображения.

С 1996 года поставляются и уже дают практические результаты системы «ПАПИЛОН» для работы с отпечатками и следами ладоней.

Разработка автоматизированных дактилоскопических систем идет по пути постоянного совершенствования версий, совершенствуется, и компьютерная техника отсюда возникает возможность создания массивов в миллион и более отпечатков. Однако здесь возникает острая проблема: с увеличением базы данных увеличивается и рекомендательный список, предоставляемый оператору для исследования.

Наиболее удачным выходом из данной ситуации было бы оснащение дежурных частей сканерами для безкрасковой прокатки (так называемыми Live skaner – живой сканер) с помощью которых можно не только изготовить электронные дактилокарты высокого качества, но и передать их за считанные минуты в любую АДИС. Такие сканеры выпускаются в России с 1993 года, фирмами «ПАПИЛОН» и «СОНДА». Однако это оснащение потребует значительных финансовых затрат, а средств выделяемых из бюджета явно не хватает.

Перспективой на ближайшее будущее в развитии автоматизированных дактилоскопических систем будет создание новой АДИС областного уровня. С 1997 года предприятиями – разработчиками АДИС «СОНДА» (г. Миасс) и НАДИС «ДАКТОМАТ» (г. Минск) начаты совместные работы в этом направлении. В фундамент проекта заложена новая система признаков дактилоскопических изображений, которая обеспечит необходимую надежность и избирательность поиска на базе данных как областного, так и федерального уровня.

Новая АДИС будет иметь многоуровневую систему, которая охватывает существующую структуру потоков дактилоскопической информации и должна соответствовать организационной структуре подразделений МВД РФ. На областном уровне это единый комплексный узел, подсистемами в который входят базы данных ИЦ, ЭКУ (ЭКО) ГУВД (УВД). В крупных городах областного подчинения могут быть организованы территориальные узлы АДИС, включающие в себя базы данных объединенных по территориальному признаку. На самом нижнем уровне – районные и межрайонные АДИС со своими локальными дактилоскопическими массивами. При наличии каналов связи система позволит организовать оперативные запросы и передачу информации как по вертикали между разноуровневыми узлами, так и по горизонтали между узлами одного уровня.

Принцип работы указанных выше АДИС применяется при разработке иных АИПС для поиска и исследования разнообразных следов-отображений: обуви, на пулях и гильзах и др. Например, АИПС «СОНДА-СЛЕД», АИПС «Арсенал-5», АЛИПС «СОНДА-ОПТЕЛ».

***АИПС «СОНДА-СЛЕД»***позволяет создавать картотеку отпечатков обуви с различных мест преступлений, а также проверку каждого вводимого следа со следами имеющимися в базе.

***АИПС «Арсенал-5»***обеспечивает хранение, просмотр, печать изображений любых следов на пулях, гильзах, объектах микроскопических исследований, автоматический поиск по первичным и вторичным следам на пулях, трассам на гильзах. Результат поиска оформляется в виде рекомендательного списка, упо­рядоченного по значениям критерия идентичности.

Для контроля результатов поисков предусмотрен просмотр и совмеще­ние на экране монитора пар изображений следов, как в соответствии с рекомендательными списками, так и в произвольном порядке. При этом со­вмещение изображений может выполняться в автоматическом режиме или вручную (подобно тому, как это делается в сравнительном микроскопе). Совмещенные изображения следов можно распечатать на принтере в качестве документального подтверждения идентичности следов. Развертка производится с помощью автофокусирующей телекамеры с высоким разрешением.

В ***АЛИПС «СОНДА-ОПТЕЛ»***используется принципиально новый метод измерения – сканирование лазерным лучом профиля объекта. Позволяет получать в наглядном виде развертку профиля трасс на пуле, картечи и дроби, следа бойка на капсуле гильзы, следов воздействия отражателя на гильзе, а также в автоматическом режиме проводить сравнительные исследования с образцами пуль и гильз проверяемого оружия и находящихся в банке данных пулегильзотеки.

Указанные АИПС являются компонентами АПК (автоматизированных программных комплексов) и АРМ (автоматизированных рабочих мест эксперта). Так, например, система «СОНДА-ОПТЕЛ» - это автоматизированное рабочее место эксперта-баллиста. В экспертной практике разработано и используется несколько АПК и АРМ, которые предназначены для определённого типа экспертных задач.

Создание автоматизированных программных комплексов и автоматизированных рабочих мест эксперта означает переход к новой, более эффективной технологии экспертных исследований.

В рассмотренных АИПС поиск хотя и осуществляется по методике криминалистической идентификации, но не устанавливает тождество объекта. Поиск заканчивается обнаружением максимально сходных объектов. Для установления тождества необходимо судебно-экспертное исследование, осуществляемое непосредственно экспертом, то есть идентификацию осуществляет лично эксперт. Иными словами, использование компьютерных технологий в судебной экспертизе не исключает личностного участия человека в исследовании в целом, в частности, в оценке его результатов. Объясняется это тем, что экспертиза является источником доказательств[[13]](#footnote-13).

### *10.3. Компьютеризация иных криминалистических учетов.*

Автоматизированные учетысостоят из ряда автоматизиро­ванных информационно-поисковых систем (АИПС).

Приведем основные АИПС и кратко охарактеризуем их на­значение и возможности.

***АИПС «Картотека»*** - автоматизированный пофамильный и дактилоскопический учет, служит для получения сведений о судимости, месте и времени отбывания наказания, дате и основании освобождения, о смерти в местах лишения сво­боды, об изменении приговора, амнистии; о месте жительства и месте работы до осуждения; о розыске лиц, задержанных за бро­дяжничество; перемещении осужденных; группе крови, дактило­скопической формуле.

***АИПС «Опознание»*** выдает информацию о лицах, про­павших без вести, неопознанных трупах, неизвестных больных и детях – гражданах Российской Федерации, СНГ и лицах без гражданства.

***АИПС «Оповещение»*** обеспечивает учет преступни­ков, госу­дарственных должников, неплатильщиков алимен­тов, пропавших без вести, отрабатывает запросы на лиц, нахо­дящихся в федеральном розыске, а также готовит циркуляры на объявление или прекращение розыска.

***АИПС «Оружие»*** позволяет вести учет утраченного и выявленного вооружения.

***АИПС «Автопоиск»*** содержит информацию о легковых и грузовых автомобилях, автобусах, полуприцепах отечественного и иностранного производства со следующими установочными дан­ными – государственный номер, номера двигателя, кузова и шас­си.

***АИПС «Антиквариат»*** выдает сведения об утраченных и выявленных предметах, представляющих историческую, художе­ственную или научную ценность. К ним относят археологические находки, предметы древности, антропологические и этнографи­ческие предметы, исторические реликвии, художественные про­изведения и предметы искусства.

***АИПС «Вещь»*** информирует пользователя о похищенных и изъятых номерных вещах, а также документах, ценных бумагах общего государственного обращения в связи с совершенными преступлениями.

***АИПС «Сейф»*** позволяет осуществлять сбор, обработку и выдачу информации о преступлениях, при совершении которых взламывались металлические хранилища.

***АИПС «Досье»*** позволяет подучить сведения об особо опас­ных рецидивистах, «ворах в законе», «авторитетах» преступного мира и др.; установочные данные, приметы, место работы, место жительства, связи, привычки и т.д.

***АИПС «Насилие»*** обеспечивает такими сведениями о тяж­ких нераскрытых и раскрытых преступлениях, связанных с наси­лием против личности, как предмет посягательства, место, время и способ совершения, описание изъятых следов и др.

***АИПС «Криминал-И»***используется для ведения учета правонарушений и преступлений, совершен­ных иностранными гражданами, лицами без гражданства (ЛГБ) и гражданами России, постоянно проживающими за границей. В АИПС функционируют пять подсистем:

1. ***«Административ­ная практика»*** несет информацию о фактах административ­ных правонарушений, допущенных иностранцами и ЛБГ на территории России;

2. ***«Преступление»*** – о тех же лицах, совер­шивших преступления;

3. ***«Дорожно-транспортное происше­ствие»*** позволяет собирать, обрабатывать, хранить и выдавать оперативно-справочную и аналитическую информацию об иностранцах и ЛБГ – участниках дорожно-транспортных происшествий;

4. ***«Розыск»*** – о находя­щихся в розыске и разысканных;

5. ***«Наказание»*** – о находя­щихся под следствием, арестованных или отбывающих нака­зание на территории России.

### 11. Компьютеризация судебной экспертизы.

### *11.1. Общие вопросы компьютеризации судебных экспертиз.*

Третье направление автоматизации расследования – компьютеризация и математизация судебной экспертизы. Первым обязательным условием применения кибернетических средств в производстве экспертиз является математическое моделирование объекта. И разработка алгоритма процесса его познания.

Развитие судебной экспертизы идёт интенсивными темпами. Научно-технический прогресс оказывает на институт судебной экспертизы чрезвычайно сильное и многостороннее влияние. Оно выражается в том, что за последние годы значительно усовершенствовалась материальная база экспертных подразделений, проводится работа по внедрению нового и развитию существующего технического, программного и технологического обеспечения для решения судебно-экспертных задач. Набирают силу процессы автоматизации и компьютеризации экспертной деятельности, позволяя экономить время и концентрироваться на более важных и значимых участках.

Направлением компьютеризации экспертиз является разработка программ при их производстве.

Проблема человек – машина не нова, по ней были высказаны различные, и в том числе диаметрально противоположные точки зрения, основные из них сводятся к следующему:

- ЭВМ необходимо передать формализуемые операции, эксперт же должен концентрироваться на творческом процессе;

- эксперту необходимо знать процесс «исследовательской деятельности»

компьютера, незнание механизма этой деятельности отнимает право эксперта применять ЭВМ при производстве экспертизы.

Однако гораздо важнее другое «надёжно ли в техническом смысле работает машина и даёт ли она верные результаты….»[[14]](#footnote-14). И здесь важную роль играют лица, разрабатывающие и реализующие программы для компьютеров (программисты, операторы и т.д.).

Работа на компьютеризированном рабочем месте эксперта осуществляется, как правило, без участия оператора, в режиме диалога.

В отношении правового положения программиста высказаны разные мнения:

1) Программисты, операторы и т.д. – технические помощники эксперта, которые обязаны контролировать их работу[[15]](#footnote-15);

2) Лица, реализующие программы для компьютеров – являются экспертами, а экспертиза является комплексной [[16]](#footnote-16).

Более точной является позиция Р.С. Белкина, который полагает, что «при использовании компьютерных программ, решающих идентификационные задачи на основании количественных оценок, если эксперт детально представляет себе математический аппарат решения данного вопроса и согласен с критериями, используемыми для количественной оценки признаков (пусть даже не им предложены эти критерии), он может отвечать за экспертные выводы единолично. Программист в этом случае выступает в роли одного из разработчиков методики. Комплексными такие экспертизы быть не могут даже тогда, когда компьютерная программа составляется специально для данной экспертизы, поскольку эксперт здесь один, а программист осуществляет создание программы по предложенному ему экспертом алгоритму. Однако, если такой алгоритм решения конкретной задачи составляется совместно экспертом и математиком, такая экспертиза может обладать всеми чертами комплексной»[[17]](#footnote-17).

Таким образом, статус лиц, разрабатывающих и реализующих программы для ЭВМ при производстве экспертизы, необходимо определить в Законе о судебной экспертизе.

В сфере экспертной деятельности автоматизированные системы могут использоваться в организации и непосредственно в исследовании следов и вещественных доказательств, а также выработке профилактических мер. И, наконец, ЭВМ используется как прибор оргтехники, при подготовке экспертных заключений. Так, система ***«РАСТР-5»***(фирма «ПАПИЛОН») предназначена для подготовки иллюстраций к заключениям и экспертизам. При этом исключается фотопроцесс, в связи, с чем повышается производительность подразделения и уменьшается время производства экспертиз. Система позволяет подготовить иллюстрации к дактилоскопическим, баллистическим, почерковедческим, трасологическим заключениям и экспертизам, к заключениям по холодному оружию, исследованию печатей и штампов и т.д.

Руководствуясь системным подходом к проблеме автоматизации рабочего места эксперта криминалиста, фирма «ПАПИЛОН» разработала комплекс ***«ВИДЕО-5»***:

- решающий проблему оперативного ввода следов в АДИС;

- решающий проблему качественной печати изображений следов и других изображений, и тем самым исключающий фотопроцесс;

- предоставляющий мощные средства быстрой обработки сложных следов, которые позволяют работать как со светлыми так и темными дактилопленками; получения негативных, а при необходимости и зеркальных изображений и т.д.

Информационный поиск в АДИС и аналогичных им системах осуществляется автома­тически. Поиск выступает в роли этапа (предварительного исследования) экспертизы. Во многих случаях это обязательный этап, без которого само исследование либо малоэффективно вследствие неопе­ративности, либо невозможно вообще из-за неразре­шимости экспертных задач.

Поиск направлен на классификацию объекта экс­пертного исследования (например, определение вида горюче-смазочных материалов, лаков, красок. Поиск осуществляется на основе положений теории криминалистической идентификации с использованием классификационных методов установления групповой принадлежности. В качестве идентифицирующего объ­екта выступают поисковые признаки исследуемого экспертом объекта и признаки объектов, введенных в банк данных АИПС.

Такой поиск имеет и негативные стороны. В от­личие от эксперта, исследующего идентифицируемый и идентифицирующий объекты и воспринимающего все их признаки в совокупности, система использует лишь те, которые введены в нее. И тут может быть несоот­ветствие по объему или характеру. Оно может повлечь обнаружение (выдачу) большого количества объектов (включая искомый). Это не влияет на истинность ко­нечного результата, но увеличивает объем экспертного исследования и время, затраченное на него (увеличивается удельный вес ручного труда), т. е. снижает эффективность исследования – конечную цель автоматизации.

Серьезным негативным последствием является «пропуск цели», когда поиск неудачен, система не об­наружит имеющийся в банке данных искомый объект.

Во избежание отмеченных негативных последст­вий важно выявить и закодировать весь комплекс идентификационных признаков. Чем полнее выявлен этот комплекс признаков и введен в систему, тем ме­нее вероятна ошибка компьютера.

### *11.2. Автоматизированные информационные системы разработанные для производства экспертиз.*

**Криминалистическая экспертиза.**

***1) Судебно-баллистическая экспертиза:***

а) ***АИПС «Оружие»*** предназначена для хранения и поиска информации по нарезному оружию. В ней содержится информация на 900 образцов отечественного и зару­бежного оружия включает две подсистемы: пистолеты и револьверы; боеприпасы. Система позволяет вво­дить данные по оружию, редактировать ранее введен­ную информацию, производить поиск по заданным ус­ловиям, а также хранить и выводить на экран графи­ческое изображение оружия и следообразующих дета­лей оружия;

б) ***АИПС «Ружье»*** предназначена для хранения и поиска информации по охотничьему и спортивному оружию, содержит информацию по 60 характеристи­кам ружей. Система позволяет вводить данные по оружию, производить поиск по заданным условиям;

в) АИПС «Арсенал-5», АЛИПС «СОНДА-ОПТЕЛ», АБИС «ТАИС-2» предназначены для идентификации огнестрельного оружия.

***Автоматизированная баллистическая иденти­фикационная система «ТАИС-02»*** предназначена для автоматического сканирования цилиндрической части боковой поверхности пули или гильзы, хранения полу­ченных видеоразверсток в создаваемой базе данных компьютера, автоматического выбора видеоизображе­ний из базы данных для последующей идентификации объектов. Компьютер автоматизирует работу, осущест­влявшуюся ранее большей частью в ручном режиме: фоторазверстку стреляной пули, сравнение её с образ­цами. Использование «ТАИС-2» позволяет уменьшить время обработки материалов при проведении экс­пертизы по сравнению с традиционными фотографиче­скими методами.

АИПС «Арсенал-5», АЛИПС «СОНДА-ОПТЕЛ» рассмотрены в лекции № 10 «Автоматизация криминалистических учетов»;

г) ***АПК «Внешняя баллистика****»* позволяет автома­тизировать экспертные исследования, сопряженные с определением возможности поражения пулей (дробью). Исследование основано на производстве расчетов: траектории снаряда, скорости снаряда на за­данном расстоянии от места выстрела, расстояния, на котором снаряд имеет заданную скорость.

***2) Дактилоскопическая экспертиза* – *АДИС «ПАПИЛОН», «СОНДА-ПЛЮС», «ПО­ИСК», «ДАКТО-ПРО», «АРМЭК»*** и др. – рассмотрены в теме «Автоматизация криминалистических учетов»;

***3) Экспертиза холодного оружия:* *система «Холодное оружие»*** содержит информа­цию о методике классификации холодного оружия, ос­новные технические параметры холодного оружия, графическую информацию. Указанная система носит обеспечивающий характер;

***4) Трасологическая экспертиза: АИПС «СОНДА-СЛЕД»***позволяет создавать картотеку отпечатков обуви с различных мест преступлений, а также проверку каждого вводимого следа со следами имеющимися в базе.

Специальные исследования.

***1)* *АПК «Газхром»*** используется для обработки хроматограмм при проведении исследований методом га­зожидкостной хроматографии. Система позволяет счи­тывать хроматограммы веществ; выводить их на экран или печатающее устройство; осуществлять количест­венные расчеты и другие операции.

***2)* *Пожарно-техническая экспертиза:* *Программный модуль «Экпотех ПМ-1»*** предна­значен для подготовки заключения эксперта по ре­зультатам исследования изъятых с места пожара проб обугленных остатков древесины, полимеров, лакокра­сочных покрытий, неорганических строительных мате­риалов, проб окалины.

Работа с программным модулем осуществляется в диалоговом режиме. Используются следующие методы исследования:

- рентгеноструктурный анализ (объекты: неорга­нические стройматериалы, окалина);

- инфракрасная спектрометрия (объекты: обго­ревшие остатки лакокрасочных покрытий, полимеров, неорганические стройматериалы);

- термический анализ (объекты: обугленная дре­весина, лакокрасочные покрытия, полимеры, неоргани­ческие стройматериалы);

- химический анализ (объекты; окалина со ста­ли);

- определение электросопротивления обугленных объектов;

- определение магнитных характеристик.

Полученная в ходе исследования информация (о распределении зон термических поражений материа­лов и конструкций, о температуре и длительности теп­лового воздействия в точках отбора проб материалов) имеет важнейшее значение для обоснованности за­ключения о местоположении очага пожара.

Компьютер самостоятельно рассчитывает проме­жуточные и конечные результаты (критерии для оцен­ки зон термических поражений, температуру, длитель­ность нагрева) по формулам, указанным в методиках.

***3) Судебно-фоноскопическая экспертиза*** пред­назначена для идентификации личности по фонограм­ме речи. Разрешает она и иные вопросы: идентифика­цию магнитофона, установление признаков монтажа, копирование фонограмм и др.

В настоящее время существует ряд компьютерных систем для фоноскопических исследований. Задачей научных разработок является реализация и развитие последних достижений речевой компьютерной техно­логии в криминалистических исследованиях.

Академией МВД РФ разработана компьютерная ***фоноскопическая система Signal Viewer (SV).*** Для решения вопросов идентификации личности по рече­вому сигналу в ней используются: 1) артикуляционные признаки – широкополосные сонограммы и гармонограммы; 2) голосовые признаки – узкополосные соно­граммы, гармонограммы и интонограммы. Эти и иные элементы экспертного исследования (амплитудные спектры и др.) используются для решения задач иден­тификации магнитофонов и исследования признаков монтажа и копирования фонограмм.

Система позволяет вести всесторонний анализ речевого сигнала. Она устроена так, что эксперту по­стоянно представлены три образа анализируемого сиг­нала: общий вид сигнала в форме динамики уровня его энергии; осциллографическое описание микросегмента сигнала и один из семи возможных специальных обра­зов сигнала, выбранный экспертом самостоятельно в зависимости от вида решаемой задачи. Сама техноло­гия работы с системой имеет определенную сложность и требует специальной подготовки эксперта.

***4) Судебно-автотехническая экспертиза.***При ее производстве используется АПК «Автоэкс», разработанный еще в 1964 г. (1-й вариант) и неоднократно усовершенствованный. Он обеспечивает наиболее высокий уровень автомати­зации экспертного исследования. В режиме диалога разрешаются вопросы, связанные с наездом на пешехода. Введенные в компьютер данные конкретного дорожно-транспортного происшествия исследуются авто­матически. Компьютер формулирует заключение экс­перта и выдает его текст.

***5) Экспертизы лакокра­сочных материалов. АИПС «Марка»***– банк данных этой системы содержит сведения о сотнях эталонных образцов с призна­ками, необходимыми для решения классификационных и идентификационных задач. В АИПС реализуется ал­горитм поиска по установлению родовой (марки) и групповой (в пределах марки) принадлежности эмали. В роли признаков выступают сведения о количествен­ных характеристиках элементного состава минераль­ной части всех марок автоэмалей, которые применяют­ся автозаводами России и бывших республик Совет­ского Союза. Поиск осуществляется путем сравнения признаков неизвестной (проверяемой) автоэмали с ра­нее известными признаками имеющихся в банке данных автоэмалей. Ответ выдается в виде машинной распечатки, реализуемой устройством печати системы.

Работа с системой осуществляется в диалоговом режиме, результаты поиска выдаются на экран монитора, а затем на устройство печати.

 12. Понятие, виды и способы совершения компьютерных преступлений.

### *12.1. Понятие и виды компьютерных преступлений.*

Термин «компьютерное преступление» стал впервые упот­ребляться в американской, а затем и другой зарубежной лите­ратуре уже в начале 60-х гг., когда стали выявляться преступ­ления, совершаемые с использованием ЭВМ. Позже этот тер­мин стал широко использоваться в практической деятельности правоохранительных органов, хотя первоначально не имел под собой ни терминологического, ни правового обоснования. В настоящее время термин «компьютерное преступление» признается большинством западных криминалистов.

В российской научной и особенно в публицистической ли­тературе употребляются самые различные понятия, касающи­еся подобного рода посягательств: компьютерные преступле­ния, коммуникационные преступления, «кибербандитизм», ин­формационные преступления, программные злоупотребления и т. д. Различие в терминологии указывает на отсутствие едино­го подхода к данной проблеме.

Вопрос о состоятельности этого понятия обсуждался и рос­сийскими юристами на очередном заседании постоянно действу­ющего межведомственного семинара на тему: «Криминалисти­ка и компьютерная преступность», организованного координа­ционным бюро по криминалистике при НИИ проблем укрепле­ния законности и правопорядка Генеральной прокуратуры и экс­портно-криминалистическим центром МВД РФ в марте 1993 г. При этом в подходе к рассмотрению данной проблемы сложи­лось две точки зрения.

Одни авторы выступили против употребления данного тер­мина, аргументируя свои возражения тем, что преступления не принято дифференцировать по виду технических средств, с помощью которых они совершаются[[18]](#footnote-18).

Другие ученые (Ляпунов Ю., Максимов В., Скормников К., Селиванов Н., Вехов В., Никифорров И. и др.) признают состоя­тельность формулировки «компьютерное преступление», так как данный термин уже воспринят как зарубежной, так и отече­ственной практикой[[19]](#footnote-19).

В УК РФ вступившем в действие с 1 января 1997 г., введены новые виды преступлений - «преступления в сфере ком­пьютерной информации», выделенные в отдельную главу. Однако сам термин «компьютерное преступление» в УК РФ отсутствует. В связи с этим в литературе предлагается разли­чать понятие «компьютерного преступления» в уголовно-правовом и криминолого-криминалистическом аспектах[[20]](#footnote-20).

Вехов В.Б считает, что компьютерным преступлением являются предусмотренные уголовным законом общественно опасные действия, совершённые с использованием средств компьютерной техники[[21]](#footnote-21).

На наш взгляд, это определение не совсем точное, поскольку съём компьютерной информации может осуществляться и без использования компьютерной техники

Более точное следующее понятие, когда под компьютерным преступлением понимаются «…предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства»[[22]](#footnote-22).

В главе 28 «Преступления в сфере компьютерной инфор­мации» УК РФ определяются следующие общественно опасные деяния в отношении средств компьютерной техники.

***1. Неправомер­ный доступ к компьютерной информации (ст. 272 УК РФ)*** – под ним следует понимать несанкционированные собственником ин­формации ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ, и манипулирование ими.

***2. Создание, использование, распространение вредоносных программ и внесение изменений в существующие программы (ст. 273 УК РФ).***

Под «программой для ЭВМ» понимается объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вы­числительных машин и других компьютерных устройств с целью получения определенного результата.

С уголовно-правовой точки зрения (ст. 273 УК РФ), программа, специально разработанная или модифици­рованная для несанкционированного собственником ин­формационной системы уничтожения, блокирования, мо­дификации либо копирования информации, нарушения обычной работы ЭВМ – ***вредоносна (она называется компьютерным вирусом).***

***Компьютерные вирусы. С программно-технической точки зрения под компьютерным вирусом понимается специальная программа, способная самопроизвольно присоединяться к дру­гим программам («заражать» их) и при запуске последних вы­полнять различные нежелательные действия: порчу файлов и каталогов (при файловой организации программной среды), ис­кажение и стирание (уничтожение) данных и информации, пе­реполнение машинной памяти и создание помех в работе ЭВМ.***

***Использование ВП*** подразумевает применение разработан­ных иным лицом ВП при эксплуатации ЭВМ и обработке информации.

***Под распространением программ ВП*** понимается предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взай­мы, включая импорт для любой из этих целей.

***3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим к ним доступ (ст. 274 УК РФ).***

Неблагоприятными последствиями этих действий является уничтожение информации, блокирование инфор­мации, модификация информации, копирование инфор­мации, нарушение работы ЭВМ.

***Уничтожение*** информации это её утрата при невозможности её восстановления или стирание её в памяти ЭВМ.

Под ***блокированием*** понимается – временная или постоян­ная невозможность осуществлять какие-либо операции над компьютерной информацией в ЭВМ как результат воздейст­вия на ЭВМ и ее элементы.

***Модификация (изменение)***компьютерной информации – это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных.

***Копирование*** компьютерной информации – это повторение и устойчивое запечатление её на машинном или ином носителе.

***Нарушение работы ЭВМ***– любая нестандартная (нештатная) ситуация с ЭВМ или её устройствами, создающая временные и устойчивые помехи их функционирования в соответствии с назначением.

### *12.2. Способы совершения компьютерных преступлений.*

***1. Неправомер­ный доступ к компьютерной информации (ст. 272 УК РФ).***

***1) Непосредственный (активный) перехват.*** Осуществляется с помощью непосредственного подключения к телекоммуника­ционному оборудованию компьютера, компьютерной системе или сети, например линии принтера или телефонному проводу канала связи, используемого для передачи данных и управляю­щих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера. В свя­зи с этим различают:

1) форсированный перехват, представляю­щий собой перехват сообщений, направляемых рабочим стан­циям (ЭВМ), имеющим неполадки в оборудовании или каналах связи;

2) перехват символов – выделение из тек­ста, набираемого пользователем на клавиатуре, зна­ков, не предусмотренных стандартным кодом данной ЭВМ;

3) перехват сообщений – несанкцио­нированное подключение специального терминала к линии свя­зи, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

***2) Электромагнитный (пассивный) перехват.*** Не все пере­хватывающие устройства требуют непосредственного подклю­чения к системе. Данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых нахо­дятся средства коммуникации, а также на значительном уда­лении от них. Так, без прямого контакта можно зафиксировать и закрепить на физический носитель электромагнитное излуче­ние, возникающее при функционировании многих средств компь­ютерной техники, включая и средства коммуникации.

***3) Аудиоперехват*** или снятие информации по виброакусти­ческому каналу. Данный способ совершения преступления яв­ляется наиболее опасным и достаточно распространенным. Защита от утечки информации по этому каналу очень сложна.

Этот способ съема информации имеет две разновидности: заходовую и беззаходовую. Первая заключается в установке инфинитивного телефона (подслушивающего устрой­ства – «таблетки», «клопа», «жучка» и т. п.) в аппаратуру средств обработки информации, в различные технические уст­ройства, на проводные коммуникационные линии (радио, телефон, телевизионный кабель, охранно-пожарной сигнализации, элек­тросеть и т. п.), а также в различные конструкции инженер­но-технических сооружений и бытовых предметов.

Вторая – беззаходовая разновидность – наиболее опасна. Заключается она в следующем. Акустические и вибрационные датчики съема информации устанавливают на инженерно-тех­нические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать речевые сигналы.

***4) Видеоперехват.*** Данный способ совершения преступления за­ключается в действиях преступника, направленных на получение требуемых данных и информации путем использования раз­личной видеооптической техники. С ее помощью преступник получает, а в некоторых случаях и фиксирует требуемую информацию и данные, которые «снимаются» дистанционно с устройств видеоотображения, бумажных носи­телей информации, с нажимаемых клавиатурных клавиш при работе пользователя.

***5) «Уборка мусора».*** Этот способ совершения преступления заключается в неправомочном использовании преступником тех­нологических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Он осуществляется в двух формах: физической и электронной. В первом случае поиск отходов сводится к внимательному осмотру содержимого мусорных корзин, баков, емкостей для технологических отходов и сбору оставленных или выброшен­ных физических носителей информации.

Электронный вариант требует просмотра, а иногда и после­дующего исследования данных, находящихся в памяти компь­ютера.

***6) «За дураком».*** Этот способ часто используется преступни­ками для проникновения в запретные зоны, как производст­венные помещения, так и электронные системы. Осуществляется путём физического проникновения. Этот вариант способа рассчитан на низкую бдительность сотрудника организации и лиц, ее охраняющих. При этом преступниками может создаваться легенда.

На таком же принципе основан и электронный вариант несанкционированного доступа. В этом случае он используется преступником из числа внутренних пользователей путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру (обычно используются так называемые «шнурки» – шлейф, изготовленные кустарным способов либо внутренняя телефонная проводка) в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, выбранной в качестве предмета посягательств; кратковременно покидает свое рабочее место, оставляя терминал или персональный компьютер в активном режиме.

***7) «За хвост».*** Этот способ съема информации заключается в следующем. Преступник подключается к линии связи законного пользователя (с использованием средств компьютерной связи и терпеливо дожидается сигнала, обозначающего конец работы перехватывает его «на себя», а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе.

***8) «Компьютерный абордаж».*** Данный способ совершения компьютерного преступления осуществляется преступником путем случайного или заранее добытого подбора абонентного номера компьютерной системы потерпевшей стороны с использовани­ем, например, обычного телефонного аппарата. После успеш­ного соединения с вызываемым абонентом и появления в голов­ном телефоне преступника специфического позывного сигнала, свидетельствующего о наличие модемного входа/выхода на вызы­ваемом абонентном номере, преступником осуществляется ме­ханическое подключение собственного модема и персонального компьютера, используемых в качестве орудия совершения пре­ступления, к каналу телефонной связи. После чего преступни­ком производится подбор кода доступа к компьютерной системе жертвы (если таковой вообще имеется) или используется зара­нее добытый код.

***9) Неспешный выбор.*** Отличительной особенностью данного способа совершения преступления является то, что преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите. Однажды обнаружив их, он может неспеша исследовать содержащуюся в системе информацию, скопировать ее на свой физический носитель и, возвращаясь к ней много раз, выбрать наиболее оптимальный предмет посягательства.

***10) «Брешь».*** В отличие от «неспешного выбора», когда про­изводится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется их конкрети­зация: определяются участки, имеющие ошибку или не­удачную логику программного строения. Выявленные таким обра­зом «бреши» могут использоваться преступником многократно, пока не будут обнаружены.

***11) «Маскарад».*** Данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя. Системы защиты средств компьютерной техники, которые не обладают функциями идентификации пользователя (например, по биометрическим параметрам; отпе­чаткам пальцев, рисунку сетчатки глаза, голосу и т. п.), оказы­ваются незащищенными от этого способа.

***12) Мистификация.*** Иногда по аналогии с ошибочными теле­фонными звонками случается так, что пользователь с терминала или персонального компьютера подключается к чьей-либо системе, будучи абсолютно уверенным в том, что он работает с нужным ему абонентом. Этим фактом и пользуется преступник, форми­руя правдоподобные ответы на запросы владельца информаци­онной системы, к которой произошло фактическое подключение, и, поддерживая это заблуждение в течение некоторого периода времени, получает при этом требуемую информацию, например коды доступа или отклик на пароль.

***13) «Аварийный».*** В этом способе преступником используется тот факт, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ (аварийный или контрольный отладчик). Принцип работы дан­ной программы заключается в том, что она позволяет достаточ­но быстро обойти все имеющиеся средства защиты информа­ции и компьютерной системы с целью получения аварийного доступа к наиболее ценным данным. Такие программы являют­ся универсальным «ключом» в руках преступника.

***14) «Склад без стен».*** Несанкционированный доступ к компь­ютерной системе в этом случае осуществляется преступником путем использования системной поломки, в результате которой возникает частичное или полное нарушение нормального ре­жима функционирования систем защиты данных.

### *2. Создание, использование, распространение вредоносных программ и внесение изменений в существующие программы (ст. 273 УК РФ).*

***1) Подмена данных*** – наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия пре­ступников в этом случае направлены на изменение или введение новых данных, которое осуществляется, как правило, при вво­де-выводе информации. В частности, данный способ соверше­ния преступления применяется для приписывания счету «чужой» истории, т. е. модификации данных в автоматизированной сис­теме банковских операций, приводящей к появлению в системе сумм, которые реально на данный счет не зачислялись.

***2) Подмена кода.*** Это частный вариант способа подмены данных. Он заключается в изменение кода данных, например бухгалтерского учета.

***3) «Люк».*** Про­изводится поиск уязвимых мест в защите компьютерной системы и в найденной «бреши» про­грамма «разрывается» и туда дополнительно преступник вво­дит одну или несколько команд. Такой «люк» «открывается» по мере необходимости, а включенные команды автоматически выполняются.

***4) «Троянский конь».*** Данный способ заключается в тайном введении в чужое программное обеспечение специально создан­ных программ, которые, попадая в информационно-вычислительные системы (обычно выдавая себя за известные сервисные про­граммы), начинают выполнять новые, не планировавшиеся за­конным владельцем действия, с одновременным сохранением прежней работоспособности системы.

***5) «Троянская матрешка».*** Является разновидностью «троянского коня». Особенность этого способа заключается в том, что во фрагмент программы потерпевшей стороны вставляются не ко­манды, собственно выполняющие незаконные операции, а ко­манды, формирующие эти команды и после выполнения своей функции самоуничтожающиеся. Иначе говоря, это программные модули-фрагменты, которые создают «троянского коня» и самоликвидируются на программном уров­не по окончании исполнения своей задачи.

***6) «Троянский червь».*** Еще одна разновидность способа «троянский конь». Данный способ совершения преступления характеризуется тем, что в алгоритм работы программы, ис­пользуемой в качестве орудия совершения преступления, на­ряду с ее основными функциями, уже рассмотренными нами выше, закладывается алгоритм действий, осуществляющих са­моразмножение, программное автоматическое воспроизводство «троянского коня».

***7) «Салями».*** Такой способ совершения преступления стал возможным лишь благодаря использованию компьютерной технологии в бухгалтерских операциях. Раньше он не использо­вался преступниками по причине его «невыгодности». Данный способ основан на методике проведения операций перебрасыва­ния на подставной счет мелочи – результата округления, которая на профессиональном бухгалтерском языке называется «салями».

***8) «Логическая бомба».*** Иногда из тактических соображений хищения удобнее всего совершать при стечении каких-либо обстоятельств, которые обязательно должны наступить. В этих случаях преступниками используется рассматриваемый способ совершения преступления, основанный на тайном внесении из­менений в программу потерпевшей стороны набора команд, которые должны сработать (или срабатывать каждый раз) при наступлении определенных обстоятельств через какое-либо время. Далее включается алгоритм программы «троянского коня».

***9) «Троянский конь»*** в электронных цепях. В отличие от «троянских коней» программных, которые представляют собой совокупность команд, внедряемых в программные средства, этот способ предполагает создание определенных логических связей в электронных цепях аппаратных средств компьютер­ной техники для автоматического выполнения незаконных ма­нипуляций по аналогии с программным способом. «Троянский конь» в электронных цепях компьютеров – очень редкий спо­соб совершения компьютерного преступления. Особенность его заключается в том, что подоб­ные преступные действия возможны лишь путем внесения кон­струкционных изменений в топологию интегральных микросхем при их заводском изготовлении.

***10) Компьютерные вирусы.***

Для понимания способа совершения преступления все вирусы можно подробно классифицировать по определенным основаниям и разбить на несколько обобщенных групп. Выделяются:

1) загрузочные (системные) вирусы (поражающие загрузоч­ные секторы машинной памяти);

2) файловые вирусы (поражающие исполняемые файлы, в том числе СОМ, EXE, SYS, ВАТ-файлы и некоторые другие);

3) комбинированные вирусы.

Вопросами научного изучения компьютерных вирусов в на­стоящее время занимается специально созданная новая наука – компьютерная вирусология. С точки зрения этой науки все программы-вирусы подразделяются на две группы, имеющие подгрупповое деление, а именно:

1) по способу заражения средств компьютерной техники ви­русы подразделяются на ***резидентные и нерезидентные;***

2) по алгоритму их строения и обнаружения на ***«вульгарный вирус»*** и ***«раздробленный вирус».***

***Резидентный вирус*** при «инфицировании» программных средств оставляет в оперативной памяти компьютерной системы потерпевшей стороны свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам за­ражения и внедряется в них. Резидентный вирус находится в памяти и является активным вплоть до выключения или пере­загрузки компьютерной системы.

***Нерезидент­ный вирус*** не заражает оперативную память и является актив­ным ограниченное время, а затем «погибает», в то время как резидентный активируется после каждого включения компью­терной системы.

***Программа «вульгарного вируса»*** написана единым блоком и достаточно легко обнаруживается специалистами в самом начале ее активных проявлений с помощью набора стандарт­ных антивирусных программных средств.

Программа «раздробленного вируса» разделена на части, на первый взгляд, неимеющие между собой логической связи. Эти части содержат инструкции, которые указывают компью­теру, как собрать их воедино, в какой последовательности, в каком случае или в какое время воссоздать «вирус» и когда размножить его (принцип «троянского коня»). Таким образом, вирус почти все время находится в «распределенном» состоя­нии, лишь на короткое время своей работы собираясь в единое целое. Как правило, создатели «вируса» указывают ему число репродукций, после достижения которого он либо вымирает, либо становится агрессивным и совершает заранее заданные незаконные манипуляции.

Наиболее часто встречаются следующие вирусные модификации.

***А) Вирусы-«спутники»*** – это вирусы, не из­меняющие программные файлы. Алгоритм работы этих вирусов состоит в том, что они создают для запускающих командных файлов файлы-спутники, имеющие то же самое имя, но с рас­ширением более высокого командного порядка. При запуске такого файла ЭВМ первым запускает файл, имеющий самый высокий уровень порядка, т. е. вирус, который затем запустит и командный файл.

***Б) Вирусы-«черви»*** – вирусы, которые распро­страняются в компьютерной сети и, так же как и вирусы-»спутники», не изменяют «родительские» программы, файлы или секторы на дисках. Они проникают в память компьютера из компьютер­ной сети и, вычисляя адреса других компьютеров, рассылают по этим адресам свои копии.

***В) «Паразитические»*** – все вирусы, которые при распро­странении своих копий обязательно изменяют содержимое программ, файлов или дисковых секторов. В эту группу относятся все вирусы, которые не являются «червями» или «спутниками».

***Г) «Студенческие»*** – крайне примитивные простые ви­русы, содержащие большое число ошибок в алгоритме их строения (безграмотно написанные) и вызывающие локальные «эпидемии».

***Д) «Вирусы-невидимки» или маскирую­щиеся вирусы,*** представляющие собой весьма совершенные про­граммы, которые при исправлении пораженных программ под­ставляют вместо себя здоровые программы или их части. Кроме того, эти вирусы при обращении к программам используют достаточно оригинальные алгоритмы, позволяющие «обманывать» антивирус­ные программы.

Способность к маскировке оказалась слабым местом «вирусов-невидимок», позволяющим легко обнаружить их наличие в про­граммной среде компьютера. Достаточно сравнить информацию о файлах, выдаваемую DOS, с фактической, содержащейся на диске: несовпадение данных однозначно говорит о наличии ви­руса, т. е. способность к маскировке демаскирует эти вирусы.

***Е) Вирусы-«призраки» (мутанты)*** – достаточно трудно обнаруживаемые самокодирующиеся вирусы, не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же вируса – «призрака» не будут иметь ни одного совпадения. Это достигается не только шифрованием ос­новного тела вируса, но и модификациями кода программы-рас­шифровщика. Иными словами, вирусы-мутанты содержат в себе алгоритмы шифровки-расшифровки, обеспечивающие то, что два экземпляра одного и того же вируса, заразившие два фай­ла, не имеют ни одной повторяющейся цепочки байт (ни одного совпадения).

***Ж) Комбинированные вирусы.*** Вирусы, имеющие отдель­ные признаки вирусов, рассмотренных нами выше, в опреде­ленной алгоритмической совокупности.

Специалисты приходят к единому мнению о том, что, по-видимому, в перспективе будут появляться принципиально новые виды «вирусов». Например, такие, как «троянский конь» в электронных цепях вирусного типа. В данном случае будет иметь место уже не вирусное программное средство, а вирус­ное микроэлектронное изделие, которым является интеграль­ная микросхема.

***З) «Асинхронная атака».*** Этот способ совершения преступления основан на со­вмещении команд двух и более пользователей, чьи программы ЭВМ выполняет одновременно (параллельно) и одной из кото­рых является программа преступника.

***11) Моделирование.*** Для совершения компьютерных преступ­лений все более характерным становится использование пре­ступником способа компьютерного моделирования: моделирования поведения устройства или системы с помощью программного обеспечения. Моделируются как те процессы, в ко­торые преступники хотят вмешаться, так и планируемые спо­собы совершения преступления. Например, так называемая «черная» или «двойная» бухгалтерия, основанная на существовании двух одновременно работающих программ автоматизированного бухгалтерского учета с взаимоперетекающими контрольными данными. В данном случае одна из них функционирует в легальном (законном) ре­жиме, а другая – в нелегальном для проведения незаконных (теневых) бухгалтерских операций. Иногда одновременно с этими программами существует и третья, которая используется только одним лицом, входящим в состав преступных групп и сообществ, выполняющим роль бухгалтера по ведению общест­венной кассы преступной группировки («общака»).

***А) Реверсивная модель.*** Разновидность способа моделиро­вания. Заключается в следующем. Создается модель конкрет­ной системы, на которую планируется совершить нападение. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных данных, подбираются максимально приближенные к действительности желаемые результаты. После чего модель совершения преступ­ных действий «прогоняется» назад, к исходной точке, и преступнику становится ясно, какие манипуляции с входными-выходными данными нужно совершить, чтобы достичь желаемого корыстного результата.

***Б) «Воздушный змей».*** Данный способ используется пре­ступником для начисления и получения незаконных избыточных денежных сумм на счетах при автоматическом пересчете руб­левых остатков за счет предварительного увеличения остаточных сумм, что достигается посредством временного переноса средств со счетов с другим кодом и их последующего возвращения на ис­ходные счета.

По мнению специалистов, управлять подобным процессом можно только с помощью компьютерной системы, используя элементы моделирования преступной ситуации.

***В) «Ловушка на живца» («подсадная утка»).*** Еще одна разновидность способа моделирования. Заключается в том, что преступником создается специальная программа, которая затем записывается на физический носитель и под любым предлогом вручается или подкидывается потерпевшей стороне с расчетом на то, что ее по каким-либо причинам заинтересует данная программа и она постарается ознакомиться с ней. Алгоритм программы построен таким образом, что при ее работе в опре­деленный момент времени автоматически моделируется сис­темная поломка компьютерной системы, на которой был запущен данный программный продукт с целью проверки его качества и работоспособности. После чего указанная программа записыва­ет данные и информацию, которые могут заинтересовать пре­ступника. После того как программа выполнила заданные ей функции, она изымается у потерпевшей стороны с использова­нием различных способов.

***12) Копирование (тиражирование).*** Этот способ совершения преступления заключается в действиях преступника, направ­ленных на незаконное копирование (тиражирование) программных средств компьютерной техники, а также топологий интегральных микросхем.

Под топологией интегральной микросхемы с уголовно-правовой точки зрения понимается зафиксированное на материальном носителе пространственно-геометрическое рас­положение совокупности элементов интегральной микросхемы (ИМС) и связей между ними, а под самой ИМС понимается микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы, элементы и связи которой неразрывно сформированы в объеме и на поверхности материала, на основе которого изготовлено изделие.

Существуют две разновидности применения преступником указанного способа. В первом случае копирование осуществляется посредством законного (санкционированного) доступа к средствам компьютерной техники, во втором – посредством несанкциони­рованного доступа с использованием способов, рассмотренных на­ми выше. В последнем случае будет иметь место применение комплексного метода совершения преступления (совокупность двух и более способов совершения преступления).

***13) Преодоление программных средств защиты.*** Этот способ является вспомогательным и предназначен для подготовки совершения компьютерного преступления. Он заключается в действиях преступника, на­правленных на умышленное преодоление программных средств защиты компьютерной техники и имеет несколько разновидностей.

***14) Незаконное создание копии ключевой дискеты.*** Является одним из способов преодоления средств защиты компьютерной техники. Осуществляется преступником путем электромагнит­ного переноса всей структуры и информации, расположенных на ключевой дискете-оригинале, защищенной от копирования программными средствами, на дискету-копию, в результате чего система защиты воспринимает копию ключевой дискеты как оригинал.

***15) Модификация кода системы защиты.*** Заключается в модификации (изменении) кода модуля системы защиты, вы­полняющего следующие функции:

1) проверку ключевой дискеты;

2) корректировку счетчика установок на жесткий магнитный диск, защищенного от копирования программного средства с ключевой дискеты;

3) проверку санкционированного запуска защищенного информационного ресурса.

Обычно модификация сводится к простому обходу кода мо­дуля, выполняющего перечисленные выше функции. В некото­рых случаях модуль подвергается существенным изменениям, позволяющим обойти проверки систем защиты. Основная задача заключается в определении логики работы модуля. Последую­щее же внесение изменений в него остается «делом техники» и не представляет особого труда для преступника, разгадавшего логику построения защиты.

***16) Моделирование обращений к ключевой дискете.*** Многие программные средства защиты информации логически исполь­зуют не прямую, как это принято, работу с контроллером, предназначенным для управления внешними (периферийными) устройствами, а средства системы BIOS – базовой системы ввода-вывода информации, пред­ставляющей собой часть программного обеспечения, входящего в состав компьютерной системы, отвечающей за тестирование и начальную загрузку, поддержание стандартного интерфейса ЭВМ с периферийными устройствами и аппаратно воплощен­ную в постоянном запоминающем устройстве (ПЗУ). Этим и пользуются преступники, программно моделируя результат обращения ЭВМ к ключевой дискете. Время преодоления защиты составляет при этом от одного дня до одной недели.

***17) Использование механизма установки/снятия программ­ных средств защиты информации.*** Используя функцию снятия защищенной программы с винчестера, можно получить возмож­ность незаконного тиражирования защищенных программных продуктов в корыстных целях. Для этого преступником осуще­ствляется следующий алгоритм действий:

1) получается санкционированный или несанкционирован­ный доступ к защищенному программному средству, располо­женному на винчестере;

2) анализируется структура размещения и содержание всех файлов (в том числе скрытых), созданных на винчестере про­граммой установки;

3) выполняется копирование защищенной программы с вин­честера (при этом восстанавливается исходный счетчик установок);

4) восстанавливаются сохраненное состояние системы и ее содержимое.

В результате всех этих действий получается ключевая дискета с исходным счетчиком установок и нелегальная копия про­граммного продукта на винчестере.

***18) Снятие системы защиты из памяти ЭВМ.*** Данный спо­соб заключается в следующем. Система защиты через опреде­ленное время автоматически загружает в память ЭВМ защи­щаемое программное средство, расшифровывает его и передает управление расшифрованному коду. В этот момент в оператив­ной памяти компьютерной системы находится полностью рас­шифрованная программа и для получения несанкционирован­ной копии остается только сохранить ее в каком-либо файле. Этим и пользуются преступники.

### 13. Защита от компьютерных преступлений.

### 3.1. Основные группы мер по предупреждению компьютерных преступлений.

Известно много мер, направленных на защиту от компьютерных преступлений. Выделим из них ***правовые, организационные и технические.***

***К правовым мерам*** следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного, гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение.

***Организационные меры*** защиты СКТ включают в себя сово­купность организационных мероприятий по подбору, проверке и инструктажу персонала, участвующего на всех стадиях ин­формационного процесса; разработке плана восстановления информационных объектов после выхода их из строя; органи­зации программно-технического обслуживания СКТ; возложе­ние дисциплинарной ответственности на лиц занимающихся обеспечением безопасности конкретных СКТ; осуществление режима секрет­ности при функционировании компьютерных систем; обеспечение режима физической охраны объектов; материально-техническому обеспечению и т. д. и т. п.

***К техническим мерам*** можно отнести следующие методы защиты средств компьютерной техники, например, защита от несанкционированного доступа, от стихийных бедствий и аварий, от хищений СКТ, саботажа, диверсий; резервирование особо важных СКТ; пра­вильная организация коммуникационных сетей и ресурсов; ус­тановка охранно-пожарной сигнализации и другие меры.

### *13.2. Правовые меры защиты от компьютерных преступлений.*

Первым шагом по защите от компьютерных преступлений можно считать принятие 23 сентября 1992 Закона РФ «О правовой охране программ для электронно-вычислительных машин и баз данных» и Закона РФ «О правовой охране топологий интегральных микросхем». Они регла­ментируют порядок установления и правовую защиту ав­торских прав на программные средства компьютерной техники и топологии интегральных микросхем.

Вторым прогрессивным шагом в этом направлении является принятие Государственной Думой и Федеральным Собранием Рос­сийской Федерации сразу двух Законов: 20 января 1995 г. – «О связи» и 25 января 1995 г. – «Об информации, информатизации и защите информации», вступивших в силу с момента их опубликования. Вышеприведенные нормативные акты позволяют регули­ровать правовые отношения в сфере информационного обмена и обработки информации, в т. ч. с использованием средств но­вых информационных технологий, например:

- дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны;

- устанавливают и закрепляют права и обязанности собст­венника на эти объекты;

- определяют правовой режим функционирования средств информационных технологий;

- определяют категории доступа определенных субъектов к конкретным видам информации;

- устанавливают категории секретности данных и информации;

- дают определение и границы правового применения тер­мина «конфиденциальная информация», а также возлагают обязанности на конкретных субъектов по ее защите от различ­ных факторов.

 Решающим законодательным аккордом по рассматриваемому кругу проблем можно считать принятие в июне 1996 г. УК РФ, устанавливающего уголовную ответственность за компьютерные преступления и выделяющего информацию в качестве объекта уголовно-правовой охраны.

### *13.3. Организационные меры защиты от компьютерных преступлений.*

Организационные мероприятия, являются важным и одним из эффективных средств защиты информации.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных преступлений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к пульту управ­ления компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских до­кументов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персо­нала, что позволяет преступнику свободно использовать ЭВМ в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответ­ствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкциони­рованного доступа к рабочей станции и ее программному обеспе­чению, которое не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной тех­ники от несанкционированного доступа;

6) отсутствие категорий допуска сотрудников к доку­ментации строгой финансовой отчетности, в т. ч. находящейся в форме машинной информации;

7) отсутствие договоров с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Применяемые в большинстве организаций системы позво­ляют обычно использование таких мер безопасности, как паро­ли, недоступность программных и информационных файлов, а также другие меры.

Для любой организации существуют два вари­анта доступа к средствам компьютерной техники, которые предопределяют комплекс защитных мероприятий.

В первом варианте организация приобретает собственную ЭВМ, которую и использует для решения своих задач, являясь ее единственным пользователем. В этом случае все вопросы компьютерной безопасности более или менее контролируемы.

Во втором случае организация становится пользователем какой-либо разветвленной коллективной компьютерной сети. Поэтому многократно возрастает и риск стать потерпевшей стороной от компьютерного преступления.

Наиболее эффективной мерой в этом направлении является введение в штатное распи­сание организации должности специалиста по компьютерной безопасности либо создание специальных отделов, исходя из конкретной ситуации.

Наличие такого отдела в организации, по оценкам специалистов, снижает вероятность совершения компьютерных преступлений вдвое. В обязательном порядке это мероприятие должно осуществляться на крупных вычисли­тельных центрах, электронных «почтовых ящиках», а также в кредитно-финансовых учреждениях и организациях. В последних долж­ны создаваться специальные отделы компьютерной безопасно­сти, которыми, как правило, руково­дит один из замести­телей начальника службы безопасности.

В функциональные обязанности указанных лиц, прежде всего, должны входить следующие позиции осуществления ор­ганизационных мер обеспечения безопасности СКТ.

1) обеспечение поддержки со стороны руководства конкрет­ной организации требований защиты СКТ;

2) разработка комплексного плана защиты информации;

3) определение приоритетных направлений защиты инфор­мации в соответствии со спецификой деятельности организации;

4) составление общей сметы расходов финансирования ох­ранных мероприятий в соответствии с разработанным;

5) определение ответственности сотрудников организации за безопасность информации в пределах установленной им компе­тенции путем заключения соответствующих договоров;

6) разработка, внедрение и контроль за исполнением раз­личного рода инструкций, правил и приказов, регламентирую­щих формы допуска, уровни секретности информации, кон­кретных лиц, допущенных к работе с секретными данными и т. п.;

7) разработка эффективных мер борьбы с нарушителями защиты СКТ.

Кроме этого, в обязательном порядке должны быть реализо­ваны следующие организационные мероприятия:

1) для всех лиц, имеющих право доступа к СКТ, должны быть определены категории допуска;

2) определена административная ответственность для лиц за сохранность и санкционированность доступа к имеющимся ин­формационным ресурсам;

3) налажен периодический системный контроль за качест­вом защиты информации посредством проведения регламент­ных работ как самим лицом, ответственным за безопасность, так и с привлечением компетентных специалистов из других организаций;

4) проведена классификация информации в соответствии с ее важностью, дифференциация на основе этого мер защиты, порядок ее охраны и уничтожения;

5) организована физическая защита СКТ.

### *13.4. Технические меры защиты от компьютерных преступлений.*

Помимо организационных мер, существенную роль в борьбе с компьютерными преступлениями могут играть также меры технического характера.

Условно их можно подразделить на три основные группы в зависимости от характера и специфики охраняемого объекта, а именно: ***аппаратные, про­граммные и комплексные.***

***Аппаратные методы*** предназначены для защиты аппарат­ных средств и средств связи компьютерной техники от неже­лательных физических воздействий на них, а также для закрытия возможных нежелательных каналов утечки конфиденциальной информации и данных, образующихся как за счет побочных электромагнитных излучений и наводок, виб­роакустических сигналов, и т.д. Практическая реализация данных методов обычно осуществляется с помощью примене­ния различных технических устройств специального назначе­ния. К ним, в частности, относятся:

1) источники бесперебойного питания аппаратуры, а также различные устройства стабилизации;

2) устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находится компьютерная техника:

3) устройства комплексной защиты телефонной связи;

4) устройства, обеспечивающие только санкционированный фи­зический доступ пользователя на охраняемые объекты СКТ;

5) устройства идентификации и фиксации терминалов и пользователей при попытках несанкционированного доступа к компьютерной сети;

6) средства охранно-пожарной сигнализации;

7) средства защиты портов компьютерной техники и т.д.

Средства защиты портов выполняют несколько защитных функций, а именно:

***1) «Сверка кода».*** Компьютер защиты порта сверяет код санкционированных пользователей с кодом в запросе. Если пользователь не идентифицирован, компьютер автоматически разрывает связь с вызывающим абонентом, это предохраняет компьютерную систему от компью­терного преступления, «за хвост».

***2) «Камуфляж».*** Некоторые средства защиты портов ка­муфлируют существование портов на линии телефонной связи путем синтезирования человеческого голоса, отвечающего на вызов абонента. Поскольку большинство персональных компью­теров имеет встроенные модемы, то таким образом защищен­ные порты для них недоступны.

***3) «Звонок навстречу».*** Данная защитная функция направ­лена против способа совершения компьютерного преступления методом «маскарад». Напомним, что этот способ заключается в том, что преступник каким-либо образом узнает код законного зарегистрированного пользователя и осуществляет с его помо­щью несанкционированный доступ к СКТ с помощью любого телефонного абонента, выдавая себя за законного пользователя. В ответ на это – средство защиты портов, в памяти которого хра­нятся не только коды доступа, но и идентификационные номера телефонов, разрывает связь и автоматически осуществляет ус­тановление связи с пользователем по второму реквизиту.

***4) Ведение автоматического «электронного журнала» дос­тупа в компьютерную систему с фиксацией основных дейст­вий пользователя (стирание, изменение, запись информации).***

***Программные методы защиты*** предназначаются для непо­средственной защиты информации по трем направлениям (уровням): а) аппаратуры; б) программного обеспечения; в) данных, а также для обеспечения должного контроля за правильностью осуществления процессов ее ввода, вывода, обработки, записи, стирания, чтения и передачи по каналам связи.

Для защиты информации при ее передаче обычно исполь­зуют различные методы ***шифрования*** данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, методы шифрования позволяют достаточно надежно скрыть смысл сообщения.

Другой подход к построению средств защиты доступа осно­ван на контроле информационных потоков и разделении субъ­ектов и объектов доступа на классы секретности.

В настоящее время специалистами выделяется четыре основ­ных способа идентификации личности пользователя, а именно:

1) по предмету, которым владеет человек;

2) по паролю, личному идентификационному коду, который вводится в ЭВМ с клавиатуры;

3) по физическим характеристикам лич­ности, присущим индивидуально только ей;

4) по электронной цифровой подписи (ЭЦП), основанной на использовании криптографической системы с открытым ключом.

Последние два способа считаются самыми перспективными и надежными в плане достоверности идентификации личности.

К первому из них относятся все существующие биометрические системы санкционированного доступа, основанные на идентифика­ции личности по таким характеристикам, как голос, размер ладо­ни, отпечатки пальцев рук, сетчатка глаза, почерк, фотоснимок и т. п.

Ко второму способу относится ЭЦП, широко используемая в зарубежных странах. Она позволяет:

- гарантировать авторство сообщения;

- реализовать юридическое заверение подписи и подлинно­сти документа, переданного по каналам радиоэлектронных коммуникаций;

- повысить защищенность данных и информации, переда­ваемых по каналам связи.

Для защиты компьютерных систем действуют также специальные подпрограммы, вызывающие самоуничтожение основной про­граммы при попытке несанкционированного просмотра содер­жимого файла с секретной информацией по аналогии действия «логической бомбы».

При рассмотрении вопросов, касающихся программной защиты информационных ресурсов выделяется проблема их ***защиты от компьютерных вирусов*** как способа совершения ком­пьютерного преступления.

Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

Однако в качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера. Корпорация Intel в 1994 году предложила перспективную технологию защиты от вирусов в компьютерных сетях. Flash-память сетевых адаптеров содержит антивирусную программу, сканирующую все системы компьютера еще до его загрузки.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано не­сколько видов специальных программ, которые позволяют обнаруживать и уничто­жать вирусы. Такие программы называются *антивирусными.*

Различают следующие виды антивирусных программ:

- программы-детекторы;

- программы-доктора или фаги;

- программы-ревизоры;

- программы-фильтры;

- программы-вакцины или иммунизаторы.

***Программы-детекторы*** осуществляют поиск характерных для конкретных вирусов параметров в оперативной памяти и файлах, при обнаружении выдают соответст­вующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

***Программы-доктора или фаги,*** а также ***программы-вакцины*** не только находят за­раженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело програм­мы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наибо­лее известные из них: Aidstest, Scan, Norton Anti-Virus, Doctor Web, AVP.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и про­граммы-доктора быстро устаревают, и требуется регулярное обновление версий.

***Программы-ревизоры*** относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных облас­тей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний про­изводят сразу после загрузки операционной системы. При сравнении проверяются длина файла, контрольная сумма файла, дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно раз­витые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии, проверяемой программы от изменений, внесенных вирусом. К числу про­грамм-ревизоров относится широко распространенная в России программа Adinf.

***Программы-фильтры или «сторожа»*** представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями СОМ, ЕХЕ;

- изменение атрибутов файла;

- прямая запись на диск по абсолютному адресу;

- запись в загрузочные сектора диска;

- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посы­лает пользователю сообщение и предлагает запретить или разрешить соответст­вующее действие. Программы-фильтры весьма полезны, так как способны обнару­жить вирус на самой ранней стадии его существования до размножения. Однако, они не «лечат» файлы и диски. К недостаткам программ-сторожей можно отне­сти их «назойливость», например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла, а также возможные конфликты с другим программным обеспечением.

***Вакцины или иммунизаторы*** – это резидентные программы, предотвращающие зараже­ние файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифи­цирует программу или диск таким образом, чтобы это не отражалось на их рабо­те, а вирус будет воспринимать их зараженными и поэтому не внедрится. В на­стоящее время программы-вакцины имеют ограниченное применение. Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничто­жение обнаруженных вирусов на каждом компьютере позволяют избежать распро­странения вирусной эпидемии на другие компьютеры.

***Основные меры по защите от вирусов.***

Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить на­дежное хранение информации на дисках, необходимо соблюдать следующие правила:

- оснастить компьютер современными антивирусными программами, например Aidstest, Doctor Web, AVP, и постоянно возобновляя версии;

- перед считыванием с дискет информации, записанной на других компьютерах, всегда проверять эти дискеты на наличие вирусов, запуская антивирусные программы компьютера;

- при переносе на компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;

- периодически проверять на наличие вирусов жесткие диски компьютера, запус­кая антивирусные программы;

- всегда защищать свои дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации;

- обязательно делать архивные копии на дискетах ценной информации;

- не оставлять в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными ви­русами;

- использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей.

Для уменьшения опасности вирусных посягательств на СКТ, по мнению специалистов, необходимо предпринять следующие ***комплексные организационно-технические методы,*** которые могут быть сокращены или расширены по своему содержанию, исхо­дя из каждой конкретной ситуации.

1. Информировать всех сотрудников учреждения, организа­ции, использующих СКТ, об опасности и возможном ущербе в случае совершения вирусного посягательства.

2. Не осуществлять неофициальные связи с другими органи­зациями. связанные с обменом программных средств.

3. Запретить сотрудникам использовать и хранить на носи­телях и в памяти ЭВМ компьютерные игры, являющиеся источ­ником повышенной опасности для безопасности компьютерных систем. Если такое запрещение не может быть обеспечено, то создать специальное игровое место или общий игровой файл, постоянно контролируемый сотрудниками службы компьютерной безопасности.

4. Предостеречь сотрудников организации от использования ПС и носителей машинной информации, имеющих происхож­дение из учебных заведений различного уровня и профиля.

5. Если в процессе работы возникнет необходимость в ис­пользовании сторонних информационных компьютерных сетей, то для этих целей необходимо в обязательном порядке выделить специальное стендовое оборудование с обязательной его изоля­цией от остальных СКТ. Все файлы, поступающие из внешней компь­ютерной сети, должны обязательно проверяться (тестироваться).

6. Создать архив копий ПС, используемых в непосредствен­ной работе организации с одно­временным исключением несанкционированного доступа к этому архиву.

7. Периодически (а в организациях, имеющих ярко выра­женную денежно-финансовую и кредитную функцию, – к концу каждого рабочего дня) проводить ревизионную проверку контрольных сумм файлов, путем их сличения с эталоном, иногда хранящимся в зашифрованном либо архивированном виде.

8. Использовать для нужд электронной почты отдельный стендовый компьютер. Тестировать файлы, полученные по электронной почте.

9. Контролировать ведение журналов операторов ЭВМ. В случае отсутствия соответствующей записи при наличии работающего сотрудника принимать дисципли­нарные меры воздействия.

11. Установить системы защиты информации на особо важ­ных ЭВМ. В обязательном порядке заактивировать на них специальные комплексные антивирусные ПС.

12. Периодически пересматривать и обновлять ПС и всю систему антивирусной защиты и правила обеспечения компью­терной безопасности.

13. Постоянно контролировать исполнение установленных пра­вил обеспечения безопасности СКТ и применять меры дисцип­линарного воздействия к лицам, сознательно или неоднократно нарушавшим их.

Общепризнано мнение о том, что профилактика любого, в том числе и компьютерного, преступления должна носить ком­плексный характер и относиться к компетенции государственных органов, а не различных коммерческих охранных структур, что имеет пока место в нашей стране. Этому учит нас и опыт зару­бежных государств, где уже с 60-х гг. (с момента совершения первого компьютерного преступления) стали серьезно заниматься этими проблемами на государственном уровне. В частности, помимо основных правовых актов, о которых мы говорили ра­нее, были предприняты и другие законодательные мероприятия, направленные на обеспечение общей безопасности информаци­онных ресурсов и возлагающие ответственность за их сохран­ность на несколько федеральных ведомств.

С позиций законодатель­ства, стержневой основой в этом направлении является Указ Президента РФ «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», направленный на усиление борьбы с организо­ванной преступностью и повышение защищенности информа­ционно-телекоммуникационных систем органов государственной власти, российских кредитно-финансовых структур, предпри­ятий и организаций.

Первым официальным документом по выполнению данного Указа можно считать Постановление правительства Российской Федерации № 608 от 26 июня 1995 г. «О сертификации средств защиты информации.

### 14. Электронная цифровая подпись.

### *14.1. Понятие, сущность электронной цифровой подписи.*

В последнее время в мире наблюдается и повышенная законодательная активность в области правового регулирования электронной цифровой подписи (ЭЦП) и Россия не является исключением, 10 января 2002 г. принят Федеральный закон «Об электронной цифровой подписи» № 1-ФЗ.

Целью на­стоящего закона является обеспечение правовых ус­ловий использования электронной цифровой подписи в электрон­ных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собст­венноручной подписи в документе на бумажном носителе.

Согласно российскому закону ЭЦП – реквизит электронного документа, предназначенный для его защиты от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Это не единственное определение ЭЦП в российском законодательстве, известны и другие. Не перечисляя их все, можно привести лишь некоторые.

ЭЦП – вид аналога собственноручной подписи, являющийся средством защиты информации, обеспечивающим возможность контроля целостности и подтверждения подлинности электронных документов. Электронная цифровая подпись позволяет подтвердить ее принадлежность зарегистрированному владельцу и является неотъемлемой частью электронного документа (пакета электронных документов.

ЭЦП – вид аналога собственноручной подписи, являющийся средством защиты информации, используемым при обмене электронными документами между Банком России и его клиентами и обеспечивающим возможность контроля целостности и подтверждения подлинности электронных документов. Электронная цифровая подпись позволяет подтвердить ее принадлежность зарегистрированному владельцу.

ЭЦП – последовательность символов, полученная в результате криптографического преобразования исходной информации, которая позволяет подтверждать целостность и неизменность этой информации, а также ее авторство.

### *14.2. Назначение электронной подписи.*

В настоящее время разработан механизм ***цифровой подписи*,** которая представляет собой дополнительную информацию, приписываемую к защищаемым данным. Цифровая подпись зависит от содержания подписываемого документа и некоего секретного элемента (ключа), которым обладает толь­ко лицо, участвующее в защищенном обмене.

Функционально электронная подпись аналогична рукопис­ной подписи и обладает её основными особенностями:

- удостоверяет, что подписанный текст исходит от лица, поста­вившего подпись;

- не дает самому этому лицу возможности отказаться от обяза­тельств, связанных с подписанным текстом; гарантирует целостность подписанного текста.

Цифровая подпись представляет собой относительно неболь­шое количество дополнительной цифровой информации, пере­даваемой вместе с подписываемым текстом.

Система ЭЦП включает две процедуры:

*-* процедуру постановки подписи;

- процедуру проверки подписи.

В процедуре постановки подписи используется секретный ключ отправителя сообщения. В процедуре проверки подписи – открытый ключ отправителя. Важнейшей особенностью систе­мы ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания.

Каждая подпись содержит следующую информацию:

- дата подписи;

- срок окончания действия ключа данной подписи;

- информация о лице, подписавшем;

идентификатор подписавшего (имя открытого ключа);

собственно цифровая подпись.

### *14.3. Основные понятия.*

К данным понятиям относятся:

***электронный документ*** *–* документ, в котором информация представлена в электронно-цифровой форме;

***электронная цифровая подпись*** *–* реквизит электронного доку­мента, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографиче­ского преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сер­тификата ключа подписи, а также установить отсутствие иска­жения информации в электронном документе;

***владелец сертификата ключа подписи*** *–* физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым клю­чом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою ЭЦП в электронных документах (подписывать электрон­ные документы);

***средства электронной цифровой подписи*** *–* аппаратные и (или) программные средства, которые обеспечивают реализацию хо­тя бы одной из следующих функций:

 - создание ЭЦП в электронном документе с использованием закрытого ключа ЭЦП;

 - подтверждение с использованием открытого ключа ЭЦП под­линности ЭЦП в электронном документе;

- создание закрытых и открытых ключей ЭЦП;

***сертификат средств электронной цифровой подписи*** *–* доку­мент на бумажном носителе, выданный в соответствии с пра­вилами системы сертификации для подтверждения соответст­вия средств ЭЦП установленным требованиям;

***закрытый ключ электронной цифровой подписи*** *–* уникальная по­следовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электрон­ных документах ЭЦП с использованием средств ЭЦП;

***открытый ключ электронной цифровой подписи*** *–* уникальная по­следовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому пользователю информационной сис­темы и предназначенная для подтверждения с использованием средств ЭЦП подлинности ЭЦП в электронном документе;

***сертификат ключа подписи*** *–* документ на бумажном носителе или электронный документ с ЭЦП уполномоченного лица, удо­стоверяющего центра, которые включают в себя открытый ключ ЭЦП и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа подписи;

 ***подтверждение подлинности электронной цифровой подписи в элек­тронном документе*** *–* положительный результат проверки со­ответствующим сертифицированным средством ЭЦП;

***пользователь сертификата ключа подписи*** *–* физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;

***информационная система общего пользования*** *–* информацион­ная система, которая открыта для использования всеми физи­ческими и юридическими лицами и в услугах которой этим лицам не может быть отказано;

***корпоративная информационная система*** *–* информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участни­ков этой информационной системы.

***Технология применения системы ЭЦП***предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей:

- секретный;

- открытый.

***Секретный ключ*** хранится абонентом в тайне и используется им для формирования ЭЦП.

***Открытый ключ*** известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа. Открытый ключ является необходимым инструментом, позволяющим проверить подлинность электронного документа и автора подписи. Открытый ключ не позволяет вычислить секретный ключ.

Для генерации пары ключей (секретного и открытого) в алго­ритмах ЭЦП, как и в асимметричных системах шифрования, используются разные математические схемы, основанные на применении однонаправленных функций.

### *14.4. Значение сертификата ключа подписи.*

При создании ключей электронных цифровых подписей для использования в информационной системе общего пользова­ния должны применяться только ***сертифицированные средства электронной цифровой подписи.***

Использование несертифицированных средств ЭЦП и создан­ных ими ключей ЭЦП в корпоративных информационных системах федеральных органов государственной власти, орга­нов государственной власти субъектов РФ и органов местного самоуправления не допускается.

Сертификат ключа подписи должен содержать следующие сведения:

- уникальный регистрационный номер сертификата ключа подпи­си, даты начала и окончания срока действия сертификата клю­ча подписи, находящегося в реестре удостоверяющего центра;

- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертифи­кат ключа подписи;

*-* открытый ключ электронной цифровой подписи; наименование средств электронной цифровой подписи, с которы­ми используется данный открытый ключ электронной цифро­вой подписи;

- наименование и место нахождения удостоверяющего центра, вы­давшего сертификат ключа подписи;

- сведения об отношениях, при осуществлении которых электрон­ный документ с электронной цифровой подписью будет иметь юридическое значение.

В случае необходимости в сертификате ключа подписи на ос­новании подтверждающих документов указываются должность (с указанием наименования и места нахождения организации, в которой установлена эта должность) и квалификация владель­ца сертификата ключа подписи, а по его заявлению в пись­менной форме – иные сведения, подтверждаемые соответст­вующими документами.

Сертификат ключа подписи должен быть внесен удостоверяю­щим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

Установлен следующий порядок хранения сертификата ключа под­писи в удостоверяющем центре:

- срок хранения сертификата ключа подписи в форме электронного документа в удостоверяющем центре определяется договором между удостоверяющим центром и владельцем сертификата ключа подписи. При этом обеспечивается доступ участников информационной системы в удостоверяющий центр для полу­чения сертификата ключа подписи;

- срок хранения сертификата ключа подписи в форме электрон­ного документа в удостоверяющем центре после аннулирова­ния сертификата ключа подписи должен быть не менее уста­новленного федеральным законом срока исковой давности для отношений, указанных в сертификате ключа подписи;

- по истечении указанного срока хранения сертификат ключа подписи исключается из реестра сертификатов ключей подпи­сей и переводится в режим архивного хранения. Срок архивно­го хранения составляет не менее чем 5 лет. Порядок выдачи копий сертификатов ключей подписей в этот период устанав­ливается в соответствии с законодательством РФ;

- сертификат ключа подписи в форме документа на бумажном носителе хранится в порядке, установленном законодательст­вом РФ об архивах и архивном деле.

### *14.5. Удостоверяющие центры.*

***Удостоверяющим центром,***выдающим сертификаты ключей подписей для использования в информационных системах об­щего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные федеральным законом. При этом удо­стоверяющий центр должен обладать необходимыми матери­альными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сер­тификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содер­жащихся в сертификатах ключей подписей.

Удостоверяющий центр выполняет следующие функции:

*-* изготавливает сертификаты ключей подписей;

- создает ключи электронных цифровых подписей по обраще­нию участников информационной системы с гарантией сохра­нения в тайне закрытого ключа электронной цифровой подписи;

- приостанавливает и возобновляет действие сертификатов клю­чей подписей, а также аннулирует их;

- ведет реестр сертификатов ключей подписей; обеспечивает его актуальность и возможность свободного доступа к нему участ­ников информационных систем;

- проверяет уникальность открытых ключей электронных циф­ровых подписей в реестре сертификатов ключей подписей и ар­хиве удостоверяющего центра;

- выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;

- осуществляет по обращениям пользователей сертификатов клю­чей подписей подтверждение подлинности электронной циф­ровой подписи в электронном документе в отношении выдан­ных им сертификатов ключей подписей;

- может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

Услуги по выдаче участникам информационных систем сертификатов ключей подписей оказываются безвозмездно.

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по от­ношению к, владельцу сертификата ключа подписи:

*-* вносить сертификат ключа подписи в реестр сертификатов клю­чей подписей;

- обеспечивать выдачу сертификата ключа подписи обратившим­ся к нему участникам информационных систем; приостанавливать действие сертификата ключа подписи по об­ращению его владельца;

- уведомлять владельца сертификата ключа подписи о фактах, которые стали известны удостоверяющему центру и которые существенным образом могут сказаться на возможности даль­нейшего использования сертификата ключа подписи.

Владелец сертификата ключа подписи обязан:

*-* не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;

- хранить в тайне закрытый ключ электронной цифровой подписи; немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

При несоблюдении этих требований возмещение причиненных вследствие этого убытков возлагается на владельца сертифика­та ключа подписи.

Удостоверяющий центр, выдавший сертификат ключа подписи, обязан аннулировать его:

- по истечении срока его действия;

- при утрате юридической силы сертификата соответствующих средств электронной цифровой подписи, используемых в ин­формационных системах общего пользования;

- в случае если удостоверяющему центру стало достоверно из­вестно о прекращении действия документа, на основании ко­торого оформлен сертификат ключа подписи;

- по заявлению в письменной форме владельца сертификата ключа подписи.

Автор:

Доцент кафедры криминалистики,

к.ю.н. \_\_\_\_\_\_\_\_\_\_\_\_ В.В. Помазанов

1. Шляхов А.Р. Предмет, задачи и система правовой кибернетики. // Основы право­вой кибернетики. М.: Изд-во Московского университета, 1977. С. 27; Полевой Н.С. Методо­логические основы правовой кибернетики. М.: Изд-во Московского университета, 1977. С. 43-62. [↑](#footnote-ref-1)
2. Батурин Ю.М. Информация общества, право и человек: Сб. Влияние научно-технического прогресса на юридическую жизнь. М.: Юридическая литература, 1988. С. 91, 92. [↑](#footnote-ref-2)
3. Венгеров А.Б. Категория «информация» в понятийном аппарате юридической науки. // Советское государство и право. 1977, № 10. С. 74. [↑](#footnote-ref-3)
4. Рассолов М.М., Элькин В.Д., Рассолов И.М. Правовая информатика и управление в сфере предпринимательства. М.: Юристъ, 1996. С. 17. [↑](#footnote-ref-4)
5. Гаврилов О.Л. Курс правовой информатики: Учебник для вузов. М.: НОРМА. 2000. С. 66. [↑](#footnote-ref-5)
6. Сидоров А.А. Проблемы организации участия специалистов в расследовании преступлений. Дисс. … канд. юрид. наук. Краснодар, 2000, С. 102. [↑](#footnote-ref-6)
7. Зеленский В.Д. Основы компьютеризации расследования. Краснодар: Изд-во Кубанского госуниверситета. 1998. С. 10. [↑](#footnote-ref-7)
8. Хмыров А.А. К теоретическим основам программирования расследования. // Тез. докл. науч.-практ. конф., посвящённой 75-летию Ростовского госуниверситета. Ростов н/Д, 1990. С. 256-258. [↑](#footnote-ref-8)
9. Зеленский В.Д. Указанная работа. С. 24. [↑](#footnote-ref-9)
10. Селиванов Н.А. Поиск аналогов по делам об убийствах. М.: Юридическая литература. 1987. [↑](#footnote-ref-10)
11. Чубукова С.Г., Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики). М.: Юридическая фирма КОНТРАКТ. 2004. С. 174-175. [↑](#footnote-ref-11)
12. Зельдес И., Леви А. Организация судебных экспертиз: практика США, проблемы России. // Российская юстиция. 1996, № 7. С. 27-28. [↑](#footnote-ref-12)
13. Зеленский В.Д. Основы компьютеризации расследования. Краснодар: Изд-во Кубанского госуниверситета. 1998. С. 60-61. [↑](#footnote-ref-13)
14. Правовая информатика и кибернетика: Учебник / Под ред. Н.С. Полевого. М.: Юридическая литература, 1993. С. 334. [↑](#footnote-ref-14)
15. Ароцкер Л.Е. Организация и процессуальные вопросы использования ЭВМ в экспертной практике. // Криминалистика и судебная экспертиза. Вып. 6. Киев, 1969. С. 189. [↑](#footnote-ref-15)
16. Эджубов Л.Г. Средства кибернетического моделирования в судебном почерковедении. // Теория и практика математического моделирования в судебно-почерковедческой экспертизе. М., 1980. С. 169. [↑](#footnote-ref-16)
17. Белкин Р.С. Курс криминалистики. Т. 3, М.: Юристъ, 1997. С. 74. [↑](#footnote-ref-17)
18. Батурин Ю. М. «Компьютерное преступление» – что за термином? // Право и информатика. / Под ред. А. П. Суханова. М.: Изд-во МГУ, 1990. С. 99; Батурин Ю. М. Проблемы компьютерного права. М.: Юридическая литература, 1991. С. 167; Курило А. П. О проблеме компьютерной безопас­ности // Научно-техническая информация. Сер. 1. Орг. и методика информ. работы. 1993. № 8. С. 7. [↑](#footnote-ref-18)
19. Селиванов Н. Проблемы борьбы с компьютерной преступностью // Закон­ность. 1993. № 8. С. 36-37; Вехов В. В. Компьютерные преступления: спосо­бы совершения и раскрытия. / Под общ. ред. акад. В. П. Смагоринского. М.: Право и Закон, 1996. С. 20; Никифоров И. В. Уголовно-правовые меры борь­бы с компьютерной преступностью и обеспечение компьютерной безопас­ности // Вестник Санкт-Петербургского университета. Сер. 6. Вып. 4. 1995. № 27. С. 94; Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9; Пособие для следователя. Расследование преступлений повышенной общественной опасности. / Под ред. Я. А. Селиванова, А. И. Дворкина. М.: ООО «Лига Разум», 1998. С. 336. [↑](#footnote-ref-19)
20. Курило А. П. Указ. соч. С. 7; Батурин Ю. М. «Компьютерное преступле­ние» - что за термином? С. 97; Вехов В. В. Указ. соч. С. 23-25; Пособие для следователя. Расследование преступлений повышенной общественной опасности. / Под ред. Н. А. Селиванова и А. И. Дворкина. С. 335. [↑](#footnote-ref-20)
21. Вехов В. В. Компьютерные преступления: спосо­бы совершения и раскрытия. / Под общ. ред. акад. В. П. Смагоринского. М.: Право и Закон, 1996. С. 24. [↑](#footnote-ref-21)
22. Селиванов Н.А. Проблемы борьбы с компьютерной преступностью. //Законность, 1993. № 8.С. 37. [↑](#footnote-ref-22)