#### ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

## по дисциплине «Информационные технологии в деятельности органов внутренних дел»

ТЕМА 1. ВВЕДЕНИЕ. ПОНЯТИЕ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. КЛАССИФИКАЦИЯ И ВИДЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

#### СОДЕРЖАНИЕ:

- 1. Концептуальные основы информационных технологий.
- 2. Понятие информационных технологий.

## ВОПРОС 1. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

#### ИНФОРМАТИЗАЦИЯ И КОМПЬЮТЕРИЗАЦИЯ ОБЩЕСТВА

Во второй половине XX века возникла необходимость решения многочисленных проблем доступа к информации, вызванных возникновением так называемого «информационного кризиса», обусловленного следующими причинами:

- возникновением противоречий между ограниченными возможностями человека по восприятию и переработке информации и существующими мощными потоками и массивами хранящейся информации;
- существованием огромного количества избыточной информации, которая затрудняет восприятие полезной для потребителя информации;
- возникновением разнообразных экономических, социальных и других барьеров, препятствующих распространению информации.

образом, создалась парадоксальная ситуация: ограниченности своих возможностей люди не могут воспользоваться в полном объеме огромным информационным потенциалом, накопленным Информационный кризис мире. поставил общество необходимостью поиска путей выхода из создавшегося положения. Широкое внедрение электронных вычислительных машин, современных средств переработки и передачи информации в различные сферы деятельности положило начало новому эволюционному процессу в общества, получившего развитии человеческого название «информатизация».

Информатизация — это процесс, обеспечивающий удовлетворение нужд и интересов граждан, общества и государства в информационных ресурсах и возможность доступа к ним посредством современных информационных технологий и развитой информационной инфраструктуры. Информатизация, основанная на базе внедрения компьютерных и телекоммуникационных технологий, представляет собой инструмент эффективного использования информации и знаний в различных областях человеческой деятельности.

В современном обществе уровень информатизации характеризует уровень социально-экономического развития государства.

### ВОПРОС 2. ПОНЯТИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Понятие «технология» в процессе эволюции общества претерпевало естественные изменения, связанные с развитием производительных сил, т.е. с новыми этапами развития общества.

Древние греки считали, что технология (гр. techne – мастерство, искусство и logos – учение) – это мастерство (искусство) делать вещи.

Сегодня считается, что результатом технологического процесса может быть не только материальный объект, но и услуга, а само это понятие рассматривается с учетом его комплексности, системности современной технологии. Технология как строго научное понятие означает комплекс научных и инженерных знаний, воплощенных в способах, приёмах труда, наборах материально-вещественных факторов производства, способах их соединения для создания какого-либо продукта или услуги.

Все сказанное относится к понятию технологии, интерпретируемому в широком смысле.

В узком смысле под технологией можно понимать набор способов, средств выбора и осуществления управляющего процесса, выделенный из множества возможных реализаций этого процесса.

Технологии управляемых процессов свойственны упорядоченность и организованность, которые противопоставляются стихийным процессам.

Цель технологии материального производства – выпуск продукции, удовлетворяющей потребности человека или системы.

Поскольку можно отметить некоторое сходство процессов обработки материальных и информационных объектов, уместна и аналогия в определении понятия информационных технологий.

Создание сложных кибернетических систем, а также развитие методов и средств анализа и реализации программного и информационного обеспечения, их функционирования с

необходимостью обусловили осознание существования и развития новых видов технологий: технологии программирования и информационной технологии.

Как и любые вновь вводимые понятия, технология программирования и информационная технология (ИТ) трактуются разными авторам по-разному.

Приведем несколько определений.

Информационная технология — это совокупность процессов сбора, передачи, переработки, хранения и доведения до пользователя информации, реализуемых на современных средствах. Информационная технология это, во-первых, совокупность процессов циркуляции и переработки информации и, во- вторых, описание этих процессов.

Информационная технология — это процесс, использующий совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта).

Информационные технологии – это технологии, ориентированные на получение, обработку и распространение (передачу) информации.

Цель информационной технологии – производство информации для ее анализа человеком и принятия на его основе решения о выполнении какого-либо действия.

Выделяют следующие основные характеристики информационной технологии:

- предметом обработки (процесса) являются данные;
- целью процесса является получение информации;
- средствами осуществления процесса являются программные, аппаратные и программно-аппаратные вычислительные комплексы;
- процессы обработки данных разделяются на операции в соответствии с данной предметной областью;
- выбор управляющих воздействий на процессы должен осуществляться лицами, принимающими решения;
- критерием оптимизации процесса являются своевременность доставки информации пользователю, ее надежность, доступность, полнота.

В современном обществе основным техническим средством переработки информации служит персональный компьютер, который существенно повлиял как на концепцию построения и использования технологических процессов, так и на качество получаемой информации. Внедрение персонального компьютера в информационную сферу и применение телекоммуникационных средств связи определили новый

этап развития информационной технологии и, как следствие, изменение ее названия за счет присоединения одного из синонимов: «новая», «компьютерная», «современная». В понятие новой информационной технологии включены также коммуникационные технологии, которые обеспечивают передачу информации разными средствами, а именно: с помощью телефона, телекоммуникаций, факса и др.

Новая информационная технология — это информационная технология с «дружественным» интерфейсом работы пользователя, использующая персональные компьютеры и телекоммуникационные средства.

Телекоммуникация – дистанционная передача данных на базе компьютерных сетей и современных технических средств связи.

Три основных принципа новой (компьютерной) технологии:

- интерактивный (диалоговый) режим работы с компьютером;
- интегрированность (стыковка, взаимосвязь) с другими программными продуктами;
- гибкость процесса изменения как данных, так и постановок задач.

#### КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Все технологии информатизации разделяются на три основных класса:

- базовые;
- прикладные;
- обеспечивающие.

Базовые технологии информатизации создают возможности решения отдельных компонентов той или иной функциональной задачи на объекте информатизации, а также служат основой формирования прикладных технологий информатизации.

К базовым технологиям информатизации относятся:

- технологии программирования, включая языки программирования;
  - телекоммуникационные технологии;
  - базы данных, в том числе специализированные;
- технологии обработки изображений (распознавание образов, компьютерная графика, визуализация информатизации);
- технологии человеко-машинного интерфейса, в том числе на естественном языке;
  - технологии распознавания речи;
  - экспертные системы;

- методы и алгоритмы параллельных вычислений;
- моделирование процессов, в том числе в реальном масштабе времени;
- моделирование ситуаций, в том числе в реальном масштабе времени;
- программные и технические технологии информационной безопасности;
- технологии хранения и обработки сверхбольших массивов информации;
  - технологии криптографии;
  - сетевые технологии предоставления информационных услуг;
  - технологии цифро-аналогового преобразования.

Прикладные технологии информатизации формируются на основе базовых и ориентированы на полную информатизацию объекта, т.е. комплексное решение функциональной задачи. Эти технологии составляют основную массу продаваемых на рынке продуктов:

- системы автоматизированного проектирования (САПР);
- автоматизированные системы управления производством (АСУП);
  - системы поддержки принятия решений (СППР);
  - географические информационные системы (ГИС);
  - системы обеспечения банковской деятельности;
  - системы автоматизации офиса;
  - мультимедиа технологии, технологии виртуальной реальности;
- системы управления процессами в реальном масштабе времени (PMB);
  - системы контроля качества;
  - системы управления запасами;
- системы управления трафиком (связь, наземный, воздушный, водный виды транспорта);
  - издательские системы;
  - медицинские информационные системы;
  - бухгалтерские системы;
  - системы автоматизации торговли;
  - системы машинного перевода;
- технологии формирования и распространения информации для средств массовой информации.

Обеспечивающие технологии информатизации создают возможность реализации технологий двух первых классов. На рынке имеются, как правило, лишь их отдельные элементы:

- современная микроэлектронная база средств вычислительной техники (BT), информатики, телекоммуникаций;
- перспективные вычислительные средства (оптические, транспьютеры, нейрокомпьютеры, компьютеры нетрадиционной архитектуры и др.);
- технологии интеграции средств информатизации и отдельных технологий в функционально ориентированные среды (открытые системы);
  - технологии организации вычислительного процесса.

## ТЕМА 2. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ.

#### СОДЕРЖАНИЕ:

- 1. Текстовый редактор и текстовый процессор.
- 2. Создание, форматирование, редактирование, рецензирование, печать документа.
  - 3. Расширенные возможности текстового процессора.
- 4. Автоматизация оформления юридических документов с помощью вставки текстовых полей, автотекста, макросов.
  - 5. Работа с большими документами.
- 6. Формат PDF: назначение, характеристика, предпосылки возникновения.
  - 7. Табличные процессоры: виды, назначение, возможности.
  - 8. Работа с таблицами как с базой данных.

# ВОПРОС 1. ТЕКСТОВЫЙ РЕДАКТОР И ТЕКСТОВЫЙ ПРОЦЕССОР

ТЕКСТОВЫЙ РЕДАКТОР — программа для работы с текстом, позволяющая создавать текст, просматривать имеющийся текст, редактировать текст.

Обрабатываемый текст может быть самым разнообразным: письмо другу, скрипт, код HTML-страницы и т.д. Это так называемый Simple Text, т.е. простой текст без форматирования, содержащий буквы, цифры, иные символы. Нельзя выделить что-либо курсивом, увеличить размер, задать цвет, гарнитуру шрифта, его кегль и начертание, вставить картинку или таблицу.

С целью предания тексту нужной формы в 1982-м году был придуман Rich Text Format, он же RTF, позволяющий выделять что угодно каким угодно способом, выбирать цвет, размер, разные шрифты, вставлять картинки. Документ с форматированным текстом содержит не только непосредственно буквы и прочие изображения, но и невидимую на экране информацию о цвете, размере и начертании всех элементов.

Например, «написанное курсивом» в документе в действительности хранится так: [{\i написанное курсивом}]. Но мы все эти фигурные скобки и метки вроде «\i» на дисплее не видим.

Простой текстовый редактор не понимает, как нужно отображать дополнительную информацию, содержащую сведения о форматировании. Поэтому файл RTF, открытый в нём, будет выглядеть как обычный текст с вышеуказанными скобками и прочими метками. Зато текстовый процессор всё это понимает правильно.

То же самое — с HTML-документами, только в таких файлах язык разметки другой, с использованием угловых скобок и несколько иных символов. К примеру, «подчёркнутое» обозначается так: <u>подчёркнутое</u>. Текстовый редактор, в отличие от процессора, покажет все эти символы вперемешку с буквами, но никакого подчёркивания не отобразит.

Таким образом, ТЕКСТОВЫЙ ПРОЦЕССОР — это текстовый редактор со значительно расширенной функциональностью, способный адекватно понимать форматированные тексты, помогающий создавать и обрабатывать сложные документы, оформленные с использованием разных стилей, со вставкой различных объектов.

Следует различать понятия «Форматированный текст» и «Формат документа».

ФОРМАТИРОВАНИЕ ДОКУМЕНТА — оформление документа, применение к нему визуальных эффектов, которые облегчают его чтение и делают его более привлекательным.

ФОРМАТ ДОКУМЕНТА — это тип файла. Файлы с документами разделяются на две категории — текстовые и бинарные.

ТЕКСТОВЫЙ ФАЙЛ содержит в себе символы ASCII (American Standard Code for Information Interchange, что-то вроде «американский стандарт кодировки для обмена информацией»). ASCII — таблица кодировки для представления десятичных цифр, латинского и национального алфавитов, знаков препинания и управляющих символов вроде перехода к новой строке. Программа для открытия файлов с символами ASCII преобразовывает байты в буквы, цифры и прочие печатные знаки на дисплее.

В БИНАРНОМ ФАЙЛЕ нули и единицы выстраиваются в последовательности, которые нужны необязательно для отображения текстов (хотя есть и такие, например, \*doc). Такие файлы используются для кодирования музыка и изображений, у каждого формата свои структурные принципы организации данных.

Текстовые файлы можно открыть в текстовом редакторе, например, без труда откроются RTF- и HTML-файлы со всей служебной информацией, управляющей форматированием. Но если нужно видеть

само оформление, а не его исходный код, тогда следует открывать документ не в редакторе, а в процессоре. Бинарные файлы в текстовом редакторе читать нельзя. Скорее всего, при попытке открытия программа просто зависнет. А если вдруг что-то и отобразится, то лишь бесполезная абракадабра. Потому что с бинарными файлам нужно работать только в текстовом процессоре. Популярными текстовыми процессорами являются Microsoft Word, OpenOffice.org Writer, AbiWord.

Не являются текстовыми процессорами продвинутые текстовые редакторы, умеющие работать с форматированным текстом, способные орфографию, понимающие гиперссылки. проверять Таковыми HTML-редакторы, множественные RTF-редакторы, являются Wordpad, входящий В состав Windows, умеющий например, обрабатывать только форматированный текст. Редактор Focus Writer может даже орфографию проверять, но является всего лишь RTFредактором.

Укажем СВОБОДНО РАСПРОСТРАНЯЕМЫЕ ТЕКСТОВЫЕ ПРОЦЕССОРЫ.

<u>Apache OpenOffice</u> — один из ведущих проектов СПО для обработки текстов, электронных таблиц, презентаций, графики, базы данных и многого другого. Доступен на многих языках и работает на всех персональных компьютерах. Позволяет сохранять данные в международном открытом формате ODF, а также открывает и сохраняет файлы других распространённых офисных пакетов.

<u>LibreOffice</u> — свободный независимый офисный пакет с открытым исходным кодом, разрабатываемый The Document Foundation как ответвление от разработки OpenOffice.org.

<u>AbiWord</u> — свободный текстовый процессор, распространяемый согласно GNU General Public License. Поддерживаемые форматы — собственный (ABW), DOC (Microsoft Word), RTF, HTML и некоторые их варианты. С помощью дополнительных плагинов возможен импорт документов таких форматов, как ODT (OpenDocument), WPD (WordPerfect), SDW (StarOffice) и других.

<u>Jarte</u> — свободный текстовый процессор, использующий движок WordPad, который является частью Windows, поэтому имеет малый вес, хорошую производительность и обеспечивает полную совместимость создаваемых документов с программами Word и WordPad.

<u>GNU TeXmacs</u> — платформа для подготовки и редактирования документов со специальными возможностями для ученых. Целью

унифицированной платформы создание системы является ДЛЯ структурированных редактирования документов c содержанием различного типа (текст, иллюстрации, математические формулы, интерактивное содержимое и т. д.). Ядро для отображения использует высококачественные алгоритмы верстки для того, чтобы пользователь получал профессионально украшенные документы, которые можно было бы распечатывать или демонстрировать с портативного компьютера.

## ВОПРОС 2. СОЗДАНИЕ, ФОРМАТИРОВАНИЕ, РЕДАКТИРОВАНИЕ, РЕЦЕНЗИРОВАНИЕ, ПЕЧАТЬ ДОКУМЕНТА

ВВОД ТЕКСТА. Основой большинства документов является текст, т.е. последовательность различных символов — прописных и строчных букв кириллицы и латиницы, цифр, знаков препинания, математических символов и др. Для быстрого ввода текста целесообразно научиться десятипальцевому "слепому" методу ввода символов.

Для представления текстов могут использоваться 256 или 65 536 символов, однако не все эти символы возможно ввести с клавиатуры компьютера. Для ввода некоторых знаков математических операций, букв греческого алфавита, денежных знаков и многих других символов используются таблицы символов. Для ввода символа его необходимо найти в таблицах и нажать клавишу {Enter}.

ВСТАВКА ИЗОБРАЖЕНИЙ, ФОРМУЛ И ДРУГИХ ОБЪЕКТОВ В ДОКУМЕНТ. Большинство современных документов содержат не только текст, но и другие объекты — изображения, формулы, таблицы, диаграммы и т. д. Текстовые процессоры позволяют вставлять в документ изображения, созданные в графических редакторах, таблицы и диаграммы, созданные в электронных таблицах, и даже звуковые и видеофайлы, созданные в соответствующих приложениях.

При решении задач по физике или математике часто необходимо вставлять формулы, которые требуют многострочного представления и использования специальных математических знаков. Для ввода формул в текстовые редакторы встроены специальные редакторы формул.

Например, набранная в редакторе MathType формула корней квадратного уравнения  $ax^2+bx+c=0$  выглядит так:  $x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ .

ФОРМАТИРОВАНИЕ ТЕКСТОВОГО ДОКУМЕНТА. WORD обеспечивает форматирование документов на пяти различных уровнях:

- на уровне символов (изменение гарнитуры, начертания, размера и цвета шрифта, межбуквенного интервала в слове, анимации и т. д.);
- на уровне абзацев (выравнивание по левому краю, по правому краю, по центру и по ширине; отступы справа и слева; отступ первой строки; отступы до и после абзаца; межстрочный интервал, управление разбивкой на страницы и т.д.);
- на уровне страниц (параметры страниц, ориентация страниц, рамка, колонтитулы первой страницы, четных и нечетных страниц и т.д.);
- на уровне разделов (формирование разделов со следующей страницы или на текущей странице, разбиение текста на колонки и т.д.);
  - на уровне документа (номера страниц, оглавление и т.д.).

АБЗАЦ — фрагмент текста, который заканчивается непечатаемым символом ¶ или фрагмент текста, процесс ввода которого заканчивается нажатием на клавишу ввода Enter. К абзацу относятся: абзац основного текста, заголовки, оглавление, списки (нумерованные и маркированные) и т.д.

Для форматирования символов применяется диалоговое окно Шрифт (Формат/Шрифт) или команды на панели инструментов форматирования. Форматирование абзацев осуществляется с помощью окна диалога Абзац, которое открывается командой Формат / Абзац. Посмотреть форматирование выделенного текста можно в области задач, выполнив команду Формат / Показать форматирование.

КОПИРОВАНИЕ, ПЕРЕМЕЩЕНИЕ И УДАЛЕНИЕ ΦΡΑΓΜΕΗΤΟΒ ДОКУМЕНТА. Редактирование документа перемещения производится путем копирования, ИЛИ удаления документа. фрагментов Выделение выделенных символов ИЛИ производится с помощью мыши или клавиш управления курсором на клавиатуре при нажатой клавише Shift.

КОПИРОВАНИЕ позволяет размножить выделенный фрагмент документа, т. е. вставить его копии в указанные места документа:

- после выделения фрагмента документа и ввода команды <Копировать> выделенная часть документа помещается в буфер обмена (специальную область памяти);
- с помощью мыши или клавиш управления курсором на клавиатуре курсор устанавливается в определенное место документа и вводится команда <Вставить>. Копируемый фрагмент документа, хранящийся в буфере обмена, помещается в указанное место;
- для многократного копирования фрагмента достаточно несколько раз повторить команду <Вставить>.

ПЕРЕМЕЩЕНИЕ позволяет вставить копии выделенного фрагмента в указанные места документа, но удаляет сам выделенный фрагмент.

УДАЛЕНИЕ позволяет удалить выделенный фрагмент.

ПОИСК И ЗАМЕНА. В процессе работы над документом иногда бывает необходимо заменить одно многократно встречающееся слово на другое. Если делать это вручную, то процесс замены отнимет много времени и сил.

К счастью, в большинстве текстовых редакторов существует операция «Найти и заменить», которая обеспечивает автоматический поиск и замену слов во всем.

ПРОВЕРКА ПРАВОПИСАНИЯ. В процессе создания документа могут быть допущены орфографические ошибки в написании слов и грамматические ошибки в построении предложений. Ошибки можно исправить, если запустить встроенную во многие текстовые редакторы систему проверки правописания, которая содержит орфографические словари и грамматические правила для нескольких языков (это позволяет исправлять ошибки в многоязычных документах). Система проверки правописания не только выделяет орфографические ошибки (красной волнистой линией) и синтаксические ошибки (зеленой волнистой линией), но предлагает исправления. Проверку И варианты ИХ правописания текстовые редакторы МОГУТ проводить как

непосредственно в процессе ввода текста, так и в готовом документе по команде пользователя.

АВТОЗАМЕНА ЧАСТЫХ ОПЕЧАТОК. В процессе ввода текста иногда допускаются опечатки (например, в начале слова случайно вводятся ДВе прописные буквы). В этом случае срабатывает функция <Автозамена>, которая автоматически исправляет такие опечатки.

Кроме того, каждый пользователь может добавить в <словарь автозамены> те слова, в которых он часто делает.

СОХРАНЕНИЕ ИСПРАВЛЕНИЙ. В процессе работы над документом могут участвовать несколько пользователей.

Исправления, вносимые каждым из них, запоминаются и могут быть просмотрены и распечатаны (вставленные фрагменты обычно отображаются подчеркнутым шрифтом синего цвета, а удаленные фрагменты — зачеркнутым шрифтом красного цвета). В процессе работы над окончательной редакцией документа может быть проведено сравнение исправлений различных авторов и принят лучший вариант.

РЕЦЕНЗИРОВАНИЕ. Текстовый редактор Microsoft Word — это не только отличный инструмент для набора и форматирования текста, но и удобнейшее средство его дальнейшего исправления и правки с помощью инструментов рецензирования. Они позволяют вставлять комментарии на полях и исправлять то, что написал автор, зачеркивая исходный текст. При этом документ со всеми исправлениями и пометками будет существовать в электронном виде, а значит, будет доступен для электронной почте, a автор документа, пересылки ПО исправления, буквально одним нажатием кнопки может их принять, а не исправлять каждую пометку вручную, или же, наоборот, отклонить, оставшись при своем мнении.

Инструменты для вставки пометок и исправлений размещены на панели инструментов <Рецензирование>. Отобразить ее можно, выбрав Вид  $\rightarrow$ Панели инструментов  $\rightarrow$  Рецензирование.

Если вдруг, читая текст, у вас возникло желание прокомментировать особо понравившийся или, наоборот, неудачный момент, вы можете воспользоваться инструментом <Примечание>. Для этого выделите нужный фрагмент текста и нажмите кнопку <Добавить примечание> на панели инструментов. В поле справа от основного текста появится окно для ввода примечания. После того, как вы набрали текст, нажмите мышкой в стороне от окна для ввода примечания.

Поле для ввода примечания отобразиться справа от текста документа.

После сохранения и повторного открытия текста, на экране фрагмент, у которого есть примечание, будет выделен другим цветом. А если навести на него мышку, можно увидеть текст примечания, его автора и время его добавления. Перемещаться между добавленными примечаниями удобно с помощью специальных кнопок, размещенных на панели инструментов <Рецензирование>.

Следующим инструментом, доступным ДЛЯ редактирования, исправления. При является режим включении ЭТОГО режима записываются все изменения, вносимые в документ. Причем, как изменения, касающиеся его содержимого (будет записано удаление и добавление текста), так и изменения формата документа (изменение шрифтов, параметров страниц и т. д.). Перейти в режим записи исправлений очень просто — достаточно дважды щелкнуть мышкой по кнопке с надписью "ИСПР", которая размещена в строке состояния текстового редактора. Второй способ: нажать на кнопку <Исправления> на панели инструментов <Рецензирование>.

В зависимости от настроек Word, исправления будут либо отображаться другим цветом, либо не отображаться вовсе, но рядом исправлением будет обязательно cкаждым размещено примечание, в котором и будет указано, какие именно изменения были внесены в документ.

Все исправления и примечания наглядно отображаются на правом поле документа

Для просмотра всех исправлений следует отобразить на экране окно просмотра изменений. Для этого необходимо нажать кнопку <Окно просмотра> на панели инструментов <Рецензирование>. В нижней части экрана отобразятся все внесенные в документ исправления и примечания.

Используя это окно можно по очереди выделять в тексте документа добавленные примечания и исправления. Для этого надо дважды щелкнуть мышкой на линии, отделяющей одно примечание от другого.

Следующим шагом после просмотра внесенных изменений будет принятие решения относительно ИХ сохранения. Для ЭТОГО <Принять предназначены списки выделенное исправление> <Отклонить выделенное исправление>. Нажав соответствующую кнопку, можно раскрыть список и выбрать нужный пункт, с помощью которого можно принять или отклонить это конкретное исправление. А выбрав пункт <Отклонить все изменения> или <Применить все изменения> можно принять решение относительно правки всего документа.

СОХРАНЕНИЕ ДОКУМЕНТА. В процессе сохранения документа необходимо, прежде всего, в иерархической файловой системе компьютера выбрать диск и папку, в которой файл документа необходимо сохранить.

Кроме того, необходимо выбрать формат файла, который определяет способ хранения текста в файле. Существуют универсальные форматы текстовых файлов, которые могут быть прочитаны большинством текстовых редакторов, и оригинальные форматы, которые используются только определенными текстовыми редакторами.

Формат ТХТ (только текст, расширение в имени файла txt) является наиболее универсальным текстовым форматом. Файлы, сохраненные в этом формате, могут быть прочитаны приложениями, работающими в различных операционных системах. Достоинством этого формата является небольшой информационный объем файлов, а недостатком то, что не сохраняются результаты форматирования текста.

Формат RTF (расширенный текстовый формат, расширение в имени файла rtf) является также универсальным форматом текстовых файлов, в котором сохраняются результаты форматирования. Недостатком этого формата является большой информационный объем файлов.

Формат DOC (документ Word, расширение в имени файла doc) является оригинальным форматом текстового редактора Microsoft Word.

В этом формате полностью сохраняются результаты форматирования. Этот формат фактически является универсальным, так как понимается практически всеми текстовыми редакторами.

Формат Web-страница (расширение в имени файла htm или html) используется для хранения Web-страниц в компьютерных сетях, так как файлы в этом формате имеют небольшой информационный объем, и при этом сохраняются результаты форматирования. Документы в этом формате создаются в Web-редакторах, а также могут сохраняться с использованием многих текстовых редакторов. Достоинством этого формата является его универсальность, так как Web-страницы могут просматриваться с использованием специализированных программ (браузеров) в любых операционных системах.

Современные текстовые редакторы обеспечивают автоматическое преобразование текстового файла из одного формата в другой при его открытии и сохранении.

ПЕЧАТЬ ДОКУМЕНТА. Перед выводом документа на печать полезно выполнить предварительный просмотр документа, это позволяет увидеть, как будет выглядеть документ, напечатанный на бумаге с использованием подключенного к компьютеру принтера.

Вид напечатанного документа (например, распределение текста по страницам) может зависеть от используемого принтера, так как могут несколько различаться шрифты, используемые в разных принтерах.

При выводе документа на печать необходимо установить параметры печати: задать номера выводимых на печать страниц, количество копий документа и др.

Кроме того, целесообразно проверить установки самого принтера:

## ВОПРОС 3. РАСШИРЕННЫЕ ВОЗМОЖНОСТИ ТЕКСТОВОГО ПРОЦЕССОРА

РАБОТА С ТАБЛИЦАМИ. Чтобы сделать в Word таблицу, надо выбрать вверху на панели поле Вставка → Таблица.

Имеется 2 способа создать таблицу:

- вставить таблицу;
- нарисовать таблицу.

### Есть ДВА ВАРИАНТА ВСТАВКИ ТАБЛИЦЫ:

- вставить таблицу, выбрав курсором на мини-таблице количество строк и столбцов;
- вставить ее, нажав кнопку под мини-таблицей. Перед вами появится всплывающее окошко, где вы сможете отрегулировать количество строк и столбцов, ширину столбцов.

Чтобы ТАБЛИЦУ НАРИСОВАТЬ, вам следует выбрать пункт <Нарисовать таблицу>. Тогда курсор мышки превратится в карандаш, и вы можете смело приниматься за рисование.

Можно сделать ПРОДОЛЖЕНИЕ ТАБЛИЦЫ. Для этого надо кликнуть по крайнему столбцу (строчке) правой кнопкой мышки и во всплывающем окне выберите Вставить → Вставить столбцы (строки...

С границами таблицы можно выполнять много операций. Можно их сделать цветными, прерывистыми, а можете вовсе сделать их невидимыми. Для этого вызывается всплывающее окно правой кнопкой мышки и выбирает пункт «Границы и заливка». В появившемся окне в первой вкладке (границы) останавливаете свой выбор на типе «Нет» — и границы убираются.

ВЫРАВНИВАНИЕ ТАБЛИЦ производится несколькими способами:

- перетаскивая границы таблицы вручную на горизонтальной линейке;
  - перетаскивая каждую границу в самой таблице;
  - настроив автоматический подбор ширины столбцов.

Имеются разные ВАРИАНТЫ ВЫРАВНИВАНИЯ ТЕКСТА в таблице.

Если для всей таблицы текст надо отформатировать одинаково, то стоит выделить всю таблицу и на главной панели инструментов настроить нужное выравнивание текста и др. так же, как это делается при работе с текстом без таблиц.

В том случае, когда текст в разных ячейках должен быть отформатирован по своему, надо выделять отдельные ячейки таблицы и для каждой из них настраивать формат текста.

Есть возможность настроить выравнивание текста в ячейках таблицы не при помощи панели инструментов, а при помощи вызываемого меню, где предлагается 9 вариантов выравнивания текста в ячейках таблицы.

Чтобы СОЕДИНИТЬ ДВЕ ТАБЛИЦЫ, необходимо выделить пустое пространство между таблицами и удалить его. После того как таблицы склеятся в одну, возможно, появится необходимость подкорректировать границы таблицы. Можно соединить две таблицы подругому, именно можно в первую таблицу добавить необходимое число ячеек, скопировать содержимое второй таблицы и вставить в первую.

Чтобы сделать РАЗРЫВ ТАБЛИЦЫ, т. е. если необходимо, чтобы таблица продолжалась со следующей страницы, поставьте курсор на строку, с которой таблица начнется после разрыва, и нажмите на сочетание клавиш CTRL + Enter.

Чтобы УБРАТЬ РАЗРЫВ ТАБЛИЦЫ, надо отобразить непечатаемые символы, двойным щелчком мышки выделить надпись <Разрыв страницы> и удалить её кнопкой Delete или Enter. После этого объедините части таблицы так, как указано выше.

Чтобы УБРАТЬ ТАБЛИЦУ, А ТЕКСТ ОСТАВИТЬ, можно схитрить, сделав границы таблицы невидимыми, что позволит сохранить форматирование в каждой ячейке. Можно действительно убрать таблицу, сохранив текст, и выбрать разделитель для текста, если нажать кнопку <Преобразовать в текст>.

ВНЕДРЕНИЕ И СВЯЗЫВАНИЕ ОБЪЕКТОВ. При работе в текстовом редакторе MS Word одной из возможностей по оформлению документов является включение в текст объектов, созданных в других приложениях. Такой объект может быть создан при помощи компьютера или введён в компьютер. Имеются разные пути получения объектов:

- ввод объекта при помощи сканера;
- создание объекта в графическом редакторе;
- создание объекта в прикладной программе;
- создание объекта встроенными средствами MS Word.

Вставленный объект можно масштабировать, снабжать рамками, обрезать и позиционировать произвольным образом. Возможности внесения изменений во вставленный графический объект определяются форматом исходного файла, хранящего вставленный объект.

Информацию или объекты, созданные в других приложениях, можно включать в документ MS Word с помощью средств связывания и внедрения. Основное различие между связыванием и внедрением состоит в способе хранения данных:

- внедренные объекты становятся частью документа MS Word;
- связанная информация сохраняется в файле источнике; документ MS Word сохраняет только сведения о месте расположения информации в файле-источнике и показывает графическое представление связанной информации.

Двойным щелчком мыши на внедренном объекте можно открыть приложение, в котором этот объект был создан, причём объект уже будет загружен в рабочую область и готов к редактированию. По возвращении в документ MS Word в документе отразятся все изменения, внесённые в объект. Можно либо внедрить уже существующий объект, файл или выделенный блок, либо создать и внедрить новый объект. Для внедрения следует использовать команду «Объект» из меню «Вставка». Доступные типы объектов содержатся в списке «Тип объекта», из которого необходимо выбрать нужный. Флажок «В виде значка» позволяет хранить в тексте не сам объект, а только его пиктограмму. Эту возможность можно использовать, если объект слишком больших размеров и его значок занимает гораздо меньше места.

После нажатия в окне <Объект> кнопки *ОК* произойдет активизация программы, работающей с объектами выбранного типа. Произведя действия по редактированию объекта, приложение в котором объект был создан, следует закрыть и вернуться в Word. Перед этим нужно обновить объект, содержащийся в документе Word. Если этого не сделать, то при закрытии приложения появится запрос: следует ли обновлять объект в документе Word. Для того чтобы обновление произошло, нужно ответить утвердительно. Обычно для этого служит кнопка <ОК>. В случае создания объекта необходимо определить в поле <Тип объекта> вкладки <Создание> диалогового окна <Вставка объекта> приложение для создания внедряемого объекта.

В случае внедрения объекта из файла необходимо указать файл в разделе «Создание из файла» диалогового окна «Вставка объекта». Флажок «Связь с файлом» позволяет установить зависимость между объектом на диске и объектом в документе. Изменения в исходном файле будут автоматически отражаться на объекте в документе Word.

Когда документ Word связывается с другим файлом, связь сохраняется в нём в форме кодов поля, идентифицирующих источник связанной информации. При этом не происходит дублирования информации из источника в документе Word. Можно создавать связи как между двумя документами Word, так и между документом и файлом, созданным в другом приложении. Однажды установив связь, можно быстро проверить и обновить информацию; можно также установить такой режим, при котором связанная информация обновляется всякий обновляется файл источника. Связывание раз, когда производится командой <Объект> меню <Вставка>. Связь с файлом устанавливается при включенном переключателе <Связать с файлом> раздела <Создать из файла> диалогового окна <Объект>.

Независимо от содержимого графического объекта предусмотрены следующие возможности для работы с объектами:

ВЫДЕЛЕНИЕ; ДЛЯ работы c графическим объектом его необходимо выделить. Для этого надо поместить указатель мыши на объект и щёлкнуть мышью. Выделенный объект помещается в рамку. Если при выделении объекта удерживать клавишу Shift, то ранее выделенные объекты останутся выделенными, таким образом, получается несколько выделенных объектов;

ПЕРЕМЕЩЕНИЕ; выделенный объект можно переместить в любое место документа, перетащив его мышью;

МАСШТАБИРОВАНИЕ; на углах и серединах сторон рамки, ограничивающей выделенный объект, имеются узелки; поместив указатель мыши на узелок, можно перетащить, сторону или угол объекта, изменив тем самым размер объекта; при перетаскивании узелка в другое положение будет отображаться размер объекта в процентах по отношению к первоначальному размеру;

РЕДАКТИРОВАНИЕ; двойной щелчок мыши по объекту активизирует программу редактирования объекта;

УДАЛЕНИЕ; выделенный объект удаляется нажатием клавиши Delete.

СОЗДАНИЕ ГРАФИЧЕСКИХ ОБЪЕКТОВ — БЛОК-СХЕМ, ОРГАНИЗАЦИОННЫХ ДИАГРАММ. Двумя основными типами изображений, используемых в документах Microsoft Word, являются графические объекты и рисунки.

ГРАФИЧЕСКИЕ ОБЪЕКТЫ в Word создаются с помощью встроенного векторного редактора. Графические объекты включают автофигуры, кривые, линии и объекты WordArt. Эти объекты являются частью документа MS Word.

РИСУНКИ подготавливаются с помощью других программ и вставляются в документ MS. Рисунок, вставленный в документ, может быть растровым (точечным) или векторным. Растровые рисунки создаются с помощью растровых графических редакторов Paint, Adobe Photoshop и других. Их можно получить сканированием фотографий или при съемке цифровыми фотоаппаратами.

При СОЗДАНИИ БЛОК-СХЕМЫ можно использовать панель инструментов <Рисование>, которая позволяет выбирать различные автофигуры, добавлять текст и многое другое. Любой набор объектов на схеме можно сгруппировать.

Воспринимать информацию, содержащуюся в документе, намного легче, если он включает диаграммы, таблицы и иллюстрации. Диаграмма Microsoft Graph (MS Graph) позволяет создавать и встраивать в тексты таблицы и диаграммы.

Чтобы встроить в Word-документ объект (диаграмму) из MS Graph, следует установить курсор в позиции вставки и вызвать команду <Объект> меню <Вставка>.

В диалоговом окне вставки объекта, в списке типов объектов нужно выбрать элемент «Диаграмма Microsoft Graph». После нажатия кнопки ОК откроется окно программы MS Graph, содержащее некоторую диаграмму:

В этом окне расположено два окна: окно таблицы и окно диаграммы.

Диаграмма, созданная в MS Graph, в любой момент соответствует данным в таблице. По своему желанию пользователь может изменить тип диаграммы. Для этого необходимо выбрать команду «Тип диаграммы» в меню «Диаграмма». В открывшемся диалоговом окне «Тип диаграммы» указать тип диаграммы (линейная, круговая и т.д.) и нажать кнопку ОК.

Может возникнуть необходимость изменить не только тип диаграммы, но и шрифт. Для изменения шрифта нужно выполнить двойной щелчок внутри легенды.

В результате на экране появится диалоговое окно <Формат легенды>, содержащее раздел <Шрифт>.

Открыв его, пользователь получит возможность выбрать гарнитуру шрифта, его кегль, начертание и т.д.

Диалоговые окна для форматирования других элементов диаграммы открываются таким же способом — двойным щелчком мыши на нужном элементе.

Чтобы вставить полученную диаграмму в Word-документ, следует щелкнуть в документе (вне диаграммы). В результате диаграмма будет вставлена в документ. Размеры диаграммы можно изменять с помощью маркеров прямо в документе.

Для изменения диаграммы нужно маркировать ее и выполнить двойной щелчок, чтобы открыть прикладную программу MS Graph. После внесения изменений и возвращения в документ все изменения отразятся в нем автоматически.

ВОПРОС 4. АВТОМАТИЗАЦИЯ ОФОРМЛЕНИЯ ЮРИДИЧЕСКИХ ДОКУМЕНТОВ С ПОМОЩЬЮ ВСТАВКИ ТЕКСТОВЫХ ПОЛЕЙ, АВТОТЕКСТА, МАКРОСОВ

При оформлении документов можно использовать многие средства MS Word — текстовые поля, автотекст, макросы.

ТЕКСТОВОЕ ПОЛЕ вводится в документ с помощью панели инструментов <Формы>, которая по умолчанию скрыта от пользователя, как и многие другие панели. Чтобы вызвать ее, следует щелкнуть правой кнопкой мыши на свободном месте в области панелей инструментов и из появившегося списка выбрать <Формы>. Можно и так: в меню <Вид>

выбрать команду «Панели инструментов» и в раскрывшемся списке доступных панелей найти и кликнуть по панели «Формы».

Кнопка <Текстовое поле> на этой панели служит для вставки в шаблон документа текстовых полей различного типа. Это может быть собственно сам текст, число, дата, время или поле формул (вычисления).

По умолчанию щелчок по этой кнопке приводит к вставке в шаблон текстового поля типа <Обычный текст>, то есть любые текстовые данные (текст, цифры, пробелы, символы). Для того, чтобы изменить тип поля, необходимо либо дважды щелкнуть на самом поле, либо щелкнуть на кнопке <Параметры поля формы>. Откроется диалоговое окно.

В поле <Текст по умолчанию> можно ввести образец текста, чтобы пользователь смог сразу же понять, что именно ему следует вводить в это поле.

Поле <Максимальная длина> позволяет ограничить количество вводимых пользователем символов.

Поле <Формат текста> предлагает установить определенное форматирование вводимого текста.

Важно не забыть установить галочку в опции <разрешить изменения>, если предполагается вводить или изменять данные в этом поле.

Часто возникает необходимость набирать фрагменты текста — названия компаний, заведений, адреса, реквизиты и др., — которые имеют очень длинное название. Эти фрагменты приходится набирать в тексте возможно не один раз. Например, в договорах это могут быть даже целые разделы, в которых присутствует неизменная часть. На их набор или копирование обычно тратиться много драгоценного времени. В некоторых текстах попадаются длинные слова типа "экзистенциальный" или "общественно-политический". Для облегчения набора в таких случаях используется функция <автозамены и автотекста> — Сервис → Параметры автозамены.

В окне автозамены наберите удобное для вас сокращение и его «расшифровку», затем нажмите кнопки Добавить и ОК. Теперь, когда вы наберете сокращенный вариант, нажмете пробел или поставите любой знак препинания, Word заменит сокращение на выбранное вами слово.

Можно ввести все падежи сокращения, и тогда вам не придется исправлять окончания после автозамены, например, об-сть = общественность, об-сти = общественность, об-стью = общественностью.

Если сокращения весьма нежелательны, например для названий, то автозамена в этом случае оказывается очень полезной. Например, вы набираете текст на русском языке, в котором очень часто встречаются слова «Windows XP», «Office 2003», «Photoshop 7.0» и подобные им, тогда имеет

смысл задать для них короткие сокращения из русских букв (например, XП для Windows XP, O3 для Office 2003, ФШ для Photoshop 7.0 и так далее). Будет сэкономлено много времени и и не будет опечаток, возникающих при неверном переключении раскладки.

В стандартном списке автозамены приведены часто встречающиеся ошибки типа «больеш» вместо «больше». Если у вас есть свои «любимые» опечатки, занесите их в этот список.

Кроме всего прочего, ее можно использовать и для быстрой вставки логотипов или другого оформления в текст. Вставьте или нарисуйте любую картинку, выделите ее, нажмите Сервис → Параметры автозамены (должен быть выделен пункт Форматированный текст) и укажите нужное сокращение.

ABTO3AMEHA ФОРМАТИРОВАННОГО TEKCTA. Если пишите учебник или методическое пособие, можно сделать так, чтобы при вводе «Й1» автоматически появлялся заголовок «Упражнения» нумерованный список, в который можно начать вводить задания. Аналогично можно вставлять выделенные особым шрифтом или цветом фона врезки, стандартные предупреждения типа «Обратите внимание», «Техническая подробность» или «Термины». Впрочем, для этих целей чаще используют автотекст — Сервис  $\rightarrow$  Параметры автозамены  $\rightarrow$ Автотекст). От автозамены он отличается тем, что не нужно запоминать сокращение — достаточно ввести первые буквы слова, и Word покажет подсказку: «Нажмите ВВОД для вставки». После нажатия Enter или F3 программа автоматически завершит слово.

АВТОТЕКСТ И СМАРТ-ТЭГИ¹ АВТОЗАМЕНЫ. В качестве сокращений автозамены лучше выбирать бессмысленные сочетания типа Й1 или ФШ, иначе автозамена часто будет срабатывать не там, где нужно. Если это произошло, достаточно нажать Ctrl+Z, Alt+Backspace или Правка → Отменить, чтобы вернуть исходное слово. В Word 2002 появилась возможность сразу же отключить замену: наведите курсор мыши на нужное слово, щелкните на появившемся под ним знаке «минус» и выберите соответствующий пункт меню.

#### ВОПРОС 5. РАБОТА С БОЛЬШИМИ ДОКУМЕНТАМИ

СОЗДАНИЕ ОГЛАВЛЕНИЯ. Многие документы требуют создания оглавления. Это можно сделать вручную, однако, в Word для этого имеются специальные средства.

 $<sup>^1</sup>$  Смарт-тэг — значок, всплывающий в процессе текстообработки рядом с курсором при прохождении указателя мыши по объекту со скрытой разметкой и открывающий контекстное меню возможных операций с отмеченным объектом

Пусть имеется уже созданный документ, в котором отдельные части имеют самостоятельные заголовки.

С самого начала документа выделяем первый заголовок, и щелкаем по выделенному участку правой кнопкой мыши. В выпадающем меню выбираем пункт Абзац.

Откроется окно Абзац. Идем на вкладку <Отступы и интервалы>. Выбираем вкладку Уровень. Самым важным заголовкам присваиваем Уровень 1. Уровень 2 оставьте на всякий случай в резерве. Не присваивайте его пока никакому заголовку. Вдруг захотите разбить главы на подглавы.

Следующему подзаголовку присваиваем Уровень 3. Если у вас все заголовки одинаковые, и подзаголовки не предусматриваются, то можете смело ставить любой уровень. Это никакой роли не играет. Вот таким образом пройдитесь по всему тексту и присвойте уровень всем вашим заголовкам.

Теперь поставьте курсор в том месте документа, где вы хотите видеть ваше оглавление, и откройте в меню Вставка  $\to$  Ссылка  $\to$  Оглавление и указатели.

В новом окне «Оглавление и указатели» перейдите на вкладку Оглавление.

Установите все галочки. Больше ничего трогать не надо. Нажмите кнопку ОК.

СОЗДАНИЕ ПРЕДМЕТНОГО УКАЗАТЕЛЯ. Создание указателя более сложное, чем создание оглавления.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ — реестр терминов, названий, фамилий, которые упоминаются в документе.

Процесс создания указателя в Word состоит из двух этапов:

- отбор слов или словосочетаний, которые должны быть включены в указатель;
  - создание указателя.

Чтобы отметить элемент текста для последующего включения его в указатель, выполните следующие действия.

Выделите текст, который вы хотите поместить в указатель. Это может быть слово, словосочетание или иной фрагмент. Выберите команду Вставка — Ссылка — Оглавление и указатели. Появится диалоговое окно «Оглавление и указатели». Щелкните на ярлыке вкладки Указатель. Щелкните на кнопке Пометить. Появится диалоговое окно «Определение элемента указателя». Выделенный в документе текст

появляется в поле <Элемент указателя основной>. Текст можно отредактировать, если есть необходимость в этом. Щелкните либо на кнопке <Пометить>, либо на кнопке <Пометить все>. Кнопка <Пометить> используется для того, чтобы пометить данное написание слова и включить его в указатель. Применяйте эту кнопку, если хотите отметить только те включения данного слова, которые, на ваш взгляд, окажут читателю максимальную пользу. Кнопка <Пометить все> заставит Word найти и отметить все включения данного слова. Применяйте этот параметр, если хотите, чтобы читатель сам решил, какие случаи использования данного термина важны, а какие — нет. Закончив, щелкните на кнопке Закрыть. Диалоговое окно <Определение Нажмите элемента указателя> исчезнет. комбинацию <Ctrl+Shift+8> или кнопку <Непечатаемые символы> на панели инструментов, чтобы отключить режим <Показывать скрытые коды>. В данном случае используйте клавишу <8>, которая находится на основной, а не на дополнительной цифровой клавиатуре.

Когда, наконец, все элементы указателя будут отмечены, переходите к его составлению. Установите курсор в той части документа, в которой должен находиться указатель. Выберите команду Вставка → Ссылка → Оглавление и указатели. Щелкните на ярлыке вкладки Указатель. Стиль указателя можно выбрать в раскрывающемся списке Форматы. В области <Образец печатного документа> вы сможете увидеть все изменения, которые будут происходить с вашим указателем. С помощью списка Колонки укажите, на сколько колонок разбить указатель. В принципе, стандартным считается использование двух колонок, однако это дело вкуса. Щелкните на кнопке ОК.

Практика показывает, что при чтении книг гораздо чаще обращаются к указателю, нежели к оглавлению. Так что позаботьтесь о том, чтобы созданные вами указатели были красивыми и аккуратными.

ВСТАВКА СНОСОК, ССЫЛОК, РАЗДЕЛОВ, КОЛОНТИТУЛОВ. При оформлении документа используются средства — сноски, ссылки, разделы, колонтитулы.

СНОСКА — помещаемые внизу полосы примечание, библиографическая ссылка, перевод иноязычного текста, связанные с основным текстом знаком сноски. Чтобы сделать сноску в Word, ставим курсор в место сноски, и переходим к окну оформления сносок в Word: Вставка → Ссылка →

Сноска. В появившемся окне Сноски выбираем нужный нам формат сносок. Тут можно выбрать положение сносок <Внизу страницы> либо <Внизу текста>, как правило, делают внизу страницы. Также можно вставить, так называемые, «концевые сноски», т.е. сноски расположенные в конце документа или раздела. Даная панель также позволяет настроить формат сносок: формат нумерации или маркера. После выбора нужного формата и нумерации, нажимаем Вставить. При этом курсор переместится в поле содержимого сноски, где нам следует ввести текст сноски.

Еще одной интересной особенностью сносок в Word является то, что они представляют собой гиперссылки на свой же текст. Так, при наведении курсора мыши на маркер сноски, всплывает подсказка с ее текстом. А при двойном клике мышью по сноске, курсор перемещается непосредственно к ее тексту, что делает работу со сносками в Word еще удобнее.

Для того чтобы удалить сноску достаточно удалить ее маркер в тексте любым из известных способов, например, выделить и нажать «Delete» или «Backspace».

ССЫЛКА — инструмент для перемещения между разделами сайта и непосредственно между самими интернет-ресурсами. С помощью него поисковые системы проводят индексацию новых элементов. Структура ссылки, или гиперссылки следующая: URL (адрес страницы, куда осуществляется перемещение) и анкор (элемент, по которому создается переход; может быть в виде URL<sup>2</sup> или изображения).

Есть несколько способов, с помощью которых ссылка на сайт может быть вставлена в документ:

- скопировать ссылку из интернет-браузера и просто вставить ее в документ;
- в разделе Вставка найти пункт Гиперссылка и нажать на него; в открывшемся окне заполнить два поля: Текст и Адрес; в первом пишем название ссылки, например «Рапорт», во второе вставляем саму ссылку; нажать ОК;
- ссылку можно ввести вручную, т.е.можно самостоятельно прописать ее, начиная с букв http и так далее, и нажать клавишу Enter; в дальнейшем, чтобы такая ссылка в Word переадресовала на указанный сайт, необходимо кликнуть по ней левой кнопкой мыши, при этом зажав клавишу Crtl; таким же образом можно делать переадресации внутри

<sup>&</sup>lt;sup>2</sup> URL - это адрес ресурса в сети

компьютера, например, в одном текстовом документе сделать ссылку на другой текст или картинку; для этого в открывшемся окне раздела Гиперссылка вместо адреса нужно выбрать конечный файл.

РАЗДЕЛ — часть документа, форматирование которой никак не связано с форматированием остального документа.

Раздел нужен для того, чтобы, например, параметр первой страницы был Книжный, а второй — Альбомный, и соответственно чтобы форматировались они не зависимо друг от друга.

Чтобы ВСТАВИТЬ РАЗДЕЛ, в открытом документе MS Word в меню <Вставка> нужно выбирать элемент <Разрыв> и щёлкнуть по нему. В появившемся окне Разрыв выбрать <Со следующей страницы> и нажать Ок. Теперь можно произвести форматирование следующих страниц независимо от форматирования предыдущих.

Чтобы УДАЛИТЬ РАЗДЕЛ, необходимо поставить курсор вначале первой строки и нажать на клавиатуре Delete.

КОЛОНТИТУЛ — заголовок (имя автора, название произведения, части, главы, параграфа и т. д.), присутствующий на всех или нескольких страницах <u>печатного издания</u>.

Документ в текстовом редакторе условно разделен на несколько областей. Текст вводится в основной (центральной) части документа, но по краям остаются пустые места, которые принято называть полями. КОЛОНТИТУЛЫ — это области, расположенные в верхнем, нижнем и боковых полях на каждой странице документа. Чаще всего колонтитулы используются для вставки номеров страниц в текст, при этом у каждую цифру самостоятельно. пользователя нет нужды ВВОДИТЬ Нумерация происходит автоматически: каждой следующей странице присваивается значение, увеличенное на единицу. В колонтитулах могут содержаться надписи: время, дата, название компании или название документа. Также в колонтитулах можно разместить графические объекты — логотип фирмы или любое другое изображение. Для вставки повторяющихся текстовых и графических объектов удобнее пользоваться колонтитулами, так как текстовой или графический объект в колонтитулах не изменяется, не сдвигается, не искажается. Отпадает необходимость вводить один и тот же текст на каждой новой странице. Когда активны

колонтитулы, основная часть документа становится недоступной для редактирования, поэтому ее вид не меняется.

Чтобы задать колонтитулы в Microsoft Word 2003 года, откройте необходимый документ, выберите на панели инструментов вкладку <Вид>, а в ней — <Колонтитулы>. В появившемся специальном поле для ввода данных введите необходимые данные. Если вы хотите проставить там дату, время или номер страницы, щелкните на панели «Вставить автотекст» и выберите нужный пункт.

Для изменения информации в колонтитулах сделайте двойной щелчок левой кнопкой мыши по полю с колонтитулом либо выберите в меню <Вид> и <Колонтитулы>. Для удаления его выделите аналогичным образом колонтитул и нажмите на клавиатуре клавишу Delete.

## ВОПРОС 6. ФОРМАТ PDF: НАЗНАЧЕНИЕ, ХАРАКТЕРИСТИКА, ПРЕДПОСЫЛКИ ВОЗНИКНОВЕНИЯ

IT-сообщество постоянно пытается стандартизировать и унифицировать каждую составляющую цифрового мира. Именно поэтому так много существует различных стандартов и спецификаций. Так же дело обстоит и с текстовым форматом. Иногда при открытии документа на другом устройстве документ может выглядеть совершенно по-иному. Чтобы этого избежать, был разработан единый формат, понятный каждому устройству, — формат pdf. Именно поэтому вся техническая документация (руководства пользователя и инструкции) представлена в формате pdf.

PDF — portable document format — был разработан компанией Adobe. С течением времени формат стал очень популярным.

В документы pdf можно встраивать не только текст и графику, но и мультимедийные файлы: музыку и видео.

Укажем неоспоримые преимущества этого формата.

СОВМЕСТИМОСТЬ. На каждом новом компьютере, как правило, уже предустановленна программа для просмотра файлов pdf. Следует отметить, что любой просмотрщик отображает файл pdf именно с теми шрифтами, с которыми он был создан. Даже если данные шрифты не

установлены на ПК. Таким образом, пользователь может просматривать и распечатывать документ pdf на любом ПК именно в том виде, в котором документ был создан.

УНИВЕРСАЛЬНОСТЬ. Сегодня разработано большое количество бесплатных программ, позволяющих открывать документ pdf на ПК с операционной системой Windows, MacOS, Linux, а также на различных мобильных платформах.

КОМПАКТНОСТЬ. Как правило, файлы pdf имеют небольшой размер, и поэтому они очень удобны для отправки их по почте в качестве вложений или как вариант хранения документов на жестком диске.

БЕЗОПАСНОСТЬ. Разработчики формата предусмотрели достаточно средств для защиты документа. Так, файл в формате pdf можно защитить паролем, и никто, кроме владельца пароля не сможет даже открыть документ. Можно, например, разрешить просмотр документа, но запретить его редактирование, копирование содержимого и даже распечатку.

PDF-файлы можно создавать, используя специальные программы, которые наделены большим набором функций, однако, как правило, большинство из этих программ платные. Кроме широко распространенного "тяжелого" пакета Adobe Acrobat, есть хорошие бесплатные аналоги. Большинство из них представляют собой виртуальные принтеры, которые выводят файл на печать не на принтер, а в создаваемый pdf файл.

Можно создать PDF-файл путем сохранения документа в pdf-формате. Такой функцией обладают наиболее известные офисные пакеты: OpenOffice и MS Office 2007. Просто при сохранении файла необходимо выбрать пункт "Сохранить как..." —> "PDF или XPS".

Если установлена более ранняя версия MS Office, то можно с сайта Microsoft бесплатно скачать надстройку "Сохранение в формате XPS или PDF".

PDF-файл можно создать путем использования интернет сервиса, например, <u>doc2pdf</u> и<u>WebPDF</u>.

Форматом pdf пользуются для защиты авторских прав. Как известно, 100% защитой не обладает ни один алгоритм, конструкция pdf не исключение. Защищенный паролем файл можно открыть с помощью программы "PDF Recover". После чего файлом можно пользоваться без ограничений.

### Укажем основные программы для работы с pdf.

### 1. Для создания и редактирования pdf файлов

Acrobat	Платная	Самый большой набор функций и инструментов. Очень высокая цена.
PDF Creator		Работает как виртуальный принтер. Есть необходимый набор пользовательских функций.
Nitro PDF Professional	Платная	Умеет создавать, редактировать, объединять, зашифровывать и конвертировать pdf-файлы.

### 2. Для просмотра pdf файлов

Adobe		Хороший и функциональный просмотрщик, однако
Reader	Бесплатно	"тяжелый", т.е. долго запускается и отнимает для
		работы много системных ресурсов.
Foxit Reader		Функционал такой же, а работает намного быстрее. Я пользуюсь этой программой.

### 3. Pdf-утилиты

Abbyy PDF Transformer	Платно	Распознает текст и картинки в документе pd конвертирует их в MS Word.			
Adolix Split & Merge PDF		Даже если pdf файлы защищены паролем, программа сможет объединить или разъединить документ.			
PDF Recover	Платно	Позволяет снять пароль с pdf файла. После чего с файлом можно делать все, что захочешь.			

### ВОПРОС 7. ТАБЛИЧНЫЕ ПРОЦЕССОРЫ: ВИДЫ, НАЗНАЧЕНИЕ, ВОЗМОЖНОСТИ

ТАБЛИЧНЫЙ ПРОЦЕССОР (ТП) — прикладная программа, предназначенная для организации табличных вычислений на компьютере.

Вычислительная таблица, которая создается с помощью ТП, называется ЭЛЕКТРОННОЙ ТАБЛИЦЕЙ.

Первый табличный процессор был создан в 1979 году, предназначался для компьютеров типа Apple II и назывался VisiCalc. В 1982 году появился табличный процессор Lotus 1-2-3, предназначенный для IBM РС. Lotus объединил в себе возможности электронных таблиц, деловую графику и некоторые функции реляционной СУБД. Практически все последующие табличные процессоры (Multiplan, QuattroPro, SuperCalc и другие) поддерживали эти три функции. Одним из самых популярных табличных процессоров сегодня является МS Excel, входящий в состав пакета Microsoft Office.

ЭЛЕКТРОННАЯ ТАБЛИЦА (ЭТ) — это своеобразная компьютерная технология организации табличных расчетов. В основе ЭТ лежит несколько главных идей.

ПЕРВАЯ ИДЕЯ — рабочее поле, структурированное по образцу шахматной доски. ЭТ, подобно шахматной доске, разделена на клетки. Строки таблицы пронумерованы числами, а столбцам присвоены буквенные имена.

	A	В	С	D	Е	F
1						
2						
3			A1+B2			
4						
5						
6						

Клетки-ячейки таблицы именуются подобно клеткам шахматной доски: A1, B2 и т. п. Данные имена называют также АДРЕСАМИ ЯЧЕЕК в таблице.

Любая прямоугольная область таблицы называется БЛОКОМ или ДИАПАЗОНОМ. Блок идентифицируется именами ячеек, расположенных в противоположных углах. Например: A1:F6 — весь фрагмент таблицы, показанный здесь.

ВТОРАЯ ИДЕЯ — в ячейках таблицы помимо текстов и чисел (как и в реляционных <u>базах данных</u>), могут помещаться вычисляющие формулы. В качестве операндов в этих формулах выступают имена ячеек таблицы. Например, в ячейке СЗ находится формула A1 + B2. Сразу после занесения формулы в ячейку табличный процессор ее вычисляет и отражает в ячейке полученное значение. При изменении значений в ячейках-операндах мгновенно происходит пересчет формул.

ТРЕТЬЯ ИДЕЯ — принцип относительной адресации. Адрес ячейки, присутствующий в формуле, обозначает ее расположение относительно ячейки, в которой записана формула. Например, формула A1 + B2 в ячейке C3 воспринимается так: содержимое ячейки, расположенной на две строки выше и на два столбца левее, сложить с содержимым ячейки, расположенной на одну строку выше и один столбец левее. При переносе этой формулы в другие ячейки, например, путем копировании, формула преобразуется, сохраняя тот же смысл относительного расположения слагаемых. Например, скопированная из ячейки C3 в ячейку C4 эта формула примет вид A2 + B3.

Для отмены действия принципа относительной адресации «\$», используется символ  $\mathbf{c}$ ПОМОЩЬЮ которого ОНЖОМ сделать неизменяемым (абсолютным) как весь адрес, так и отдельную его часть (строку или столбец). Например, если в ячейке ВЗ записана формула \$A\$1+\$B\$1, то при копировании в ячейку C4 она не изменится.

Функции табличных процессоров весьма разнообразны:

- создание и редактирование электронных таблиц;
- создание многотабличных документов;
- оформление и печать электронных таблиц;

- построение диаграмм, их модификация и решение экономических задач графическими методами;
- создание многотабличных документов, объединенных формулами;
- работа с электронными таблицами как с базами данных: сортировка таблиц, выборка данных по запросам;
  - создание итоговых и сводных таблиц;
- использование при построении таблиц информации из внешних баз данных;
  - создание слайд-шоу;
  - решение оптимизационных задач;
- решение экономических задач типа "что если" путем подбора параметров;
- разработка макрокоманд, настройка среды под потребности пользователя и т.д.

Наиболее популярными электронными таблицами для персональных компьютеров являются табличные процессоры Microsoft Excel, Quattro Pro, Lotus 1-2-3 и SuperCalc. И если после своего появления в 1982 году Lotus 1-2-3 был фактически эталоном для разработчиков электронных таблиц, то в настоящее время он утратил свои лидирующие позиции. Результаты тестирования продемонстрировали явное преимущество Excel по многим параметрам. Единственное превосходство Lotus 1-2-3 — это скорость работы, но опять же, превышение небольшое.

Перспективные направления в разработке электронных таблиц основными фирмами-разработчиками определены по-разному. Фирма Microsoft уделяет особое внимание совершенствованию набора функциональных средств Excel, и в этом ее пакет явно лидирует среди всех электронных таблиц. Фирма Lotus основные усилия сконцентрировала на разработке инструментов групповой работы. Пакет Quattro Pro в результате тестирования получил достаточно высокие оценки, но ни одна из особенностей пакета не вызвала к себе повышенного внимания. Наиболее привлекательными оказались лишь возможности сортировки данных.

Ситуация, сложившаяся на рынке электронных таблиц, в настоящее время характеризуется явным лидирующим положением фирмы Microsoft — 80% всех пользователей электронных таблиц предпочитают Excel. На втором месте по объему продаж — Lotus 1-2-3, затем Quattro Pro. Доля

других электронных таблиц, например SuperCalc, совершенно незначительна.

QUATTRO PRO. Среди имеющихся на рынке электронных таблиц для DOS программа Quattro Pro лучшая. Пакет Quattro Pro рассчитан практически на любую вычислительную систему — от машин с процессором 8088 и емкостью памяти 512 Кбайт до IBM PC 486 с большой оперативной памятью.

В новой версии в верхней части экрана находится программируемое "быстрое меню", один из пунктов которого позволяет переключаться между графическим и текстовым режимами.

Табличный процессор Quattro Pro обладает рядом достоинств:

- удобный пользовательский интерфейс, дающий возможность предоставления данных в самой нестандартной форме;
  - многооконный режим работы;
- доступ к любым неограниченным по размерам внешним базам данных созданных на основе наиболее популярных СУБД;
  - хорошее качество печати входных документов;
- легкость создания программы обработки информации в таблицах, удобные средства отладки и редактирования созданных программ и т.д.

Одной из отличительных особенностей процессора Quattro Pro являются аналитические графики, которые позволяют применять к исходным данным агрегирование, вычислять скользящее среднее и проводить регрессионный анализ; результаты перечисленных действий отражаются на графиках. Набор встроенных функций в пакете Quattro Pro включает в себя все стандартные функции. Новыми для данной версии поддержка дополнительных библиотек *(a)*-функций, является разработанных независимыми поставщиками. Данный пакет включает программы линейного И нелинейного программирования. Оптимизационную модель можно записать на рабочий лист и работать с нею.

Кроме обычных команд работы с базами данных, Quattro Pro умеет читать внешние Базы в форматах Paradox, dBase и Reflex, и искать в них нужную информацию.

SUPERCALC. Основное применение SuperCalc — выполнение расчетов. Однако в силу своей гибкости он позволяет решать большинство финансовых и административных задач:

- прогнозирование продаж, роста доходов;
- анализ процентных ставок и налогов;
- учет денежных чеков;
- подготовка финансовых деклараций и балансовых таблиц;
- бюджетные и статистические расчеты;
- объединение таблиц;
- сметные калькуляции.

SuperCalc выполняет арифметические, статистические, логические, специальные функции. Он имеет дополнительные возможности: поиск и сортировка в таблицах. SuperCalc имеет довольно большие графические возможности, позволяя строить на экране семь видов диаграмм и графиков, облегчая тем самым труд пользователя.

Таблицы SuperCalc могут иметь до 9999 строк и до 127 столбцов. Строки идентифицируются числами от 1 до 9999, а столбцы буквами от А до DW.

По умолчанию в памяти ЭВМ резервируется место для 2000 строк и 127 столбцов.

Ширина каждого столбца по умолчанию устанавливается равной 9 печатным позициям, но можно установить любую ширину столбца, внеся специальную команду. На экране существует активная клетка, которая всегда подсвечивается.

Такая подсветка называется табличным курсором, который можно перемещать с помощью клавиатуры.

На экране дисплея в каждый момент можно наблюдать только 20 строк таблицы и 8 столбцов стандартной ширины.

Под двадцатой строкой размещаются так называемые служебные строки:

- 1 строка состояния (STATUS LINE), где автоматически отображаются содержимое, координаты активной клетки и др.;
- 2 строка подсказки (PROMPT LINE), где высвечивается информация об ошибках;

- 3 строка ввода (ENTRY LINE), где высвечиваются символы, набираемые на клавиатуре;
- 4 строка помощи (HELP LINE). Она показывает назначение отдельных клавиш на клавиатуре ЭВМ.

При работе в SuperCalc выделяют три основных режима работы:

- режим электронной таблицы; здесь активен только табличный курсор; редактирующий курсор неподвижен и находится в исходной позиции строки ввода;
- режим ввода; он устанавливается автоматически, с началом работы на клавиатуре;
- командный режим устанавливается несколькими способами; Наиболее распространенный способ перед набором команды нажимается команда с символом "\".

EXCEL. MS Excel — одна из самых популярных сегодня программ электронных таблиц. Ею пользуются ученые и деловые люди, бухгалтеры и журналисты, с ее помощью ведут разнообразные таблицы, списки и каталоги, составляют финансовые и статистические отчеты, подсчитывают состояние торгового предприятия, обрабатывают результаты научного эксперимента, ведут учет, ГОТОВЯТ презентационные материалы. Возможности Excel очень высоки. Обработка текста, управление базами данных — программа настолько мощна, что во многих случаях превосходит специализированные программы-редакторы или программы баз данных. Такое многообразие функций может поначалу запутать, чем заставить применять на практике. Но по мере приобретения опыта начинаешь по достоинству ценить то, что границ возможностей Excel тяжело достичь.

За многолетнюю историю табличных расчётов с применением персональных компьютеров требования пользователей к подобным программам существенно изменились. В начале основной акцент в такой программе, как, например, VisiCalc, ставился на счётные функции. Сегодня наряду с инженерными и бухгалтерскими расчетами организация и графическое изображение данных приобретают все возрастающее значение. Кроме того, многообразие функций, предлагаемое такой расчетной и графической программой, не должно осложнять работу пользователя. Программы для Windows создают для этого идеальные предпосылки. В последнее время многие как раз перешли на использование Windows в качестве своей пользовательской среды. Как следствие, многие

фирмы, создающие программное обеспечение, начали предлагать большое количество программ под Windows.

Программа Excel обеспечивает как легкость при обращении с данными, так и их сохранность. Excel позволяет быстро выполнить работу, для которой не нужно затрачивать много бумаги и времени, а также привлекать профессиональных бухгалтеров и финансистов.

Данная программа сумеет вычислить суммы по строкам и столбцам таблиц, посчитать среднее арифметическое, банковский процент или дисперсию, здесь вообще можно использовать множество стандартных функций: финансовых, математических, логических, статистических.

ТИПЫ ДАННЫХ. Так как Excel — программа, работающая с таблицами, то здесь оперируют различными данными. В электронных таблицах используют, как правило, следующие типы данных:

ТЕКСТ — любая последовательность символов;

ЧИСЛО — числовая константа;

ФОРМУЛА — выражение, состоящее из числовых величин и арифметических операций;

ФУНКЦИЯ — запрограммированные формулы, позволяющие проводить часто встречающиеся последовательности вычислений.

ОКНО EXCEL. Оформление таблиц может быть самым разнообразным, возможности форматирования данных — как в хорошем текстовом процессоре: можно менять шрифты, начертания, выделять строки, столбцы или отдельные ячейки текста цветом, рамочками и линеечками, закрашивать области фоном или цветом, строить по табличным данным графики и диаграммы, вставлять таблицу с картинками и т. д.

Программа достаточно мощная, возможности ее, особенно в последних версиях, весьма обширны. Одних только математических, логических, бухгалтерских, статистических функций, которые Excel может выполнять над табличными данными более 200.

Ехсеl — программа многооконная, что позволяет нам одновременно загружать столько файлов, сколько позволит объем оперативной памяти компьютера. Окно Excel содержит множество различных элементов. Некоторые из них присущи всем программам в среде Windows, остальные есть только в окне Excel. Вся рабочая область окна Excel занята чистым рабочим листом (или таблицей), разделённым на отдельные ячейки. Вы можете представить рабочий лист в виде отдельного окна со своим собственным заголовком — это окно называется окном рабочей книги, так как в таком окне можно обрабатывать несколько рабочих листов. На одной рабочей странице в распоряжении будет 256 столбцов и 16384 строки. Строки пронумерованы от 1 до 16384, столбцы названы буквами и комбинациями букв. После 26 букв алфавита колонки следуют комбинации букв АА, АВ и т.д.

После запуска Excel содержит пять областей:

- окно книги, которое занимает большую часть экрана;
- строку меню;
- две или больше панелей инструментов;
- строку формул и строку состояния.

Все вместе эти пять областей называются РАБОЧЕЙ ОБЛАСТЬЮ Excel.

После запуска Excel первой пока еще пустой книги дается имя Книга 1. Если в течении текущего сеанса работы будет открыта новая книга, то Excel назовет ее Книга 2. Книга Excel может содержать листы пяти типов: рабочие листы, листы диаграмм, модули Visual Basic, листы диалогов и листы макросов Microsoft Excel.

Окно книги составляет основную часть рабочей области. В нижней части окна книги размещаются кнопки прокрутки ярлыков листов, а в верхней части — строка заголовка. Новая книга первоначально содержит 16 отдельных листов.

Чтобы просмотреть содержание книги, можно использовать четыре кнопки, расположенные в нижнем левом углу окна. Две средние кнопки служат для прокрутки на один лист влево или вправо. Две крайние кнопки выполняют прокрутку к первому или последнему листу книги. Перечисленные кнопки прокрутки не активизируют листы книги. Чтобы сделать лист активным, следует после прокрутки ярлыков щелкнуть на

листе. В правом конце строки заголовка окна книги находятся три кнопки для управления размерами окон: Свернуть, Развернуть и Закрыть.

Ячейка, находящаяся на пересечении строки и столбца, является основным элементом любого рабочего листа. Каждая ячейка занимает уникальное место на листе, может хранить и отображать информацию, имеет однозначные координаты, которые называются адресом ячейки или ссылкой. Например, ячейка, находящаяся на пересечении столбца А и строки 1, имеет адрес А1. Ячейка на пересечении столбца Z и строки 100 имеет адрес Z100. Ссылки, являющиеся идентификаторами ячеек, бывают трех видов: абсолютные, относительные и смешанные. Абсолютные не изменяются, когда ячейки содержат формулы при копировании. В относительных ссылках адреса при копировании формул в другое место изменяются. Смешанные ссылки состоят из абсолютных и относительных. В тех случаях, когда необходимо, чтобы изменились координаты ячеек используют относительные ссылки, если необходимо, чтобы координаты не изменялись, используют относительную ссылку, в иных случаях используют смешанные. В тех случаях, когда координаты следует делать, неизменными перед ними ставят знак "\$". Выделенную ячейку называют активной или текущей ячейкой, адрес активной ячейки выводится в поле имени, которое находится в левом конце строки формул. При 256 столбцах и 16384 строках рабочий лист содержит более 4 миллионов ячеек.

В окне Excel, как и в других программах под Windows, под заголовком окна находится строка меню. Она содержит девять пунктов: Файл, Правка, Вид, Вставка, Формат, Сервис, Данные, Окно и Справка. Некоторые команды меню выделены обычным шрифтом (черным цветом), а некоторые выглядят блекло (серый цвет). Excel отслеживает состояние рабочего листа и позволяет выбрать только те команды, которые могут быть использованы в данной ситуации. Команды, представленные черным цветом, доступны для использования, а выделенные серым — недоступны.

Для некоторых команд в меню имеется список дополнительных команд, называемый подчиненным меню или подменю. Контекстное меню содержит только те команды, которые могут применятся к элементу, для которого активизировано меню. Контекстное меню обеспечивает удобный и быстрый доступ к нужным командам. Чуть ниже находятся панели инструментов, они значительно облегчают работу в Excel, позволяя оперативно, за счет быстрого доступа, использовать ту или иную функцию. В нижней части рабочей области Excel находится строка с ярлыками

листов, позволяющая то в каком листе мы в данный момент находимся. Под строкой ярлыков находится строка состояния, которая отражает состояние программы в момент работы с Excel.

ФУНКЦИИ EXCEL. Программа Excel содержит множество всевозможных функций. Наиболее обще их можно представить следующим образом:

ФИНАНСОВАЯ — здесь множество специальных функций, вычисляющих проценты по вкладу или кредиту, амортизационные отчисления, норму прибыли и самые разнообразные обратные и родственные величины;

ДАТА И ВРЕМЯ — большинство ее функций ведает преобразованиями даты и времени в различные форматы; Две специальные функции Сегодня и Дата вставляют в ячейку текущую дату (первая) и время (вторая), обновляя их при каждом вызове файла или при внесении любых изменений в таблицу; Такую ячейку необходимо иметь в бланках счетов, самых свежих прайс-листах, каких-нибудь типовых договорах;

ПРОСМОТР И ССЫЛКА — здесь находятся функции, позволяющие обратиться к массиву данных и получить из него самую разнообразную информацию — номера столбцов и строк, в него входящих, их количество, содержимое нужного вам элемента массива, найти, в какой ячейке этого массива находится число или текст.

МАТЕМАТИЧЕСКАЯ — вычисление математической величины: косинуса, логарифма и т.д.;

СТАТИСТИЧЕСКАЯ — общие функции использующиеся для вычисления средних значений наибольшего и наименьшего из числа для расчета распределения Стьюдента;

ССЫЛКИ И МАССИВЫ — вычисляют ссылки и массивы, значение диапазона, создание гипперссылки для сетевых и Web документов;

ТЕКСТОВЫЕ — преобразование текстов в верхние и нижние регистры, образует символы, объединяет некоторые строки и т. д.;

ЛОГИЧЕСКИЕ — вычисления выражения, выяснения значения истина или ложь;

ПРОВЕРКА СВОЙСТВ И ЗНАЧЕНИЙ — возвращение из Excel в Windows информации о текущем статусе ячейки, объекта или среды;

ПЕЧАТЬ — в Excel задаются не только горизонтальная, но вертикальная линия разбиения, что немаловажно при широких таблицах, которые вы хотели бы потом склеить. Маркеры в виде пунктирных линий появятся выше и левее активной ячейки: они более жирнее и лучше различимы, чем маркеры мягкого разбиения. Чтобы убрать лишний маркер, нужно поставить курсор ниже или правее его и выбрать команду <Убрать конец страницы> из меню Вставка.

На страничке Поля диалогового окна Параметры страницы задается верхний и нижний боковые отступы, расположения таблицы на листе, а также местоположение колонтитула.

Страничка Колонтитулы предоставляет возможность задать колонтитулы.

На страничке Лист можно указать программе, что линии сетки заголовки строк и столбцов печатать не следует. Здесь же задается область печати, интервал или список.

В закладке Страница можно задать вертикальное или горизонтальное расположение таблиц на странице и масштаб. Excel позволяет печатать увеличенные или уменьшенные копии, когда таблица слишком широкая и не помещается на страницах, даже при ландшафтном расположении.

## СОЗДАНИЕ, ФОРМАТИРОВАНИЕ, РЕДАКТИРОВАНИЕ ТАБЛИЦ

ВВОД И РЕДАКТИРОВАНИЕ ДАННЫХ. Для ввода информации в заданную ячейку нужно установить на нее курсор или нажать мышью на этой ячейке. После этого можно начинать вводить данные. С вводом первого символа вы переходите в режим ввода, при этом в строке формулы дублируется текстовая информация вводимая в ячейку а в строке состояния отображается слово Ввод.

Строка формулы Microsoft Excel, используется для ввода или редактирования значений или формул в ячейках или диаграммах. Здесь выводится постоянное значение или формула активной ячейки. Для ввода данных выделите ячейку, введите данные и щелкните по кнопке с зеленой

«галочкой» или нажмите ENTER. Данные появляются в строке формул по мере их набора.

Поле имени находится в левом конце строки ввода. Используйте поле имени для задания имен активной ячейке или выделенному блоку. Для этого щелкните на поле имени, введите туда имя и нажмите ENTER. Такие имена можно использовать при написании формул или при построении диаграмм. Также поле имени можно использовать для перехода к поименованной ячейке или блоку. Для этого откройте список и выберите из него нужное имя.

Если информация уже введена в ячейку и нужно лишь добавить или скорректировать ранее введенные данные, дважды нажмите мышью на нужной ячейке или нажмите клавишу F2, когда требуемая ячейка выделена. При этом вы переходите в режим ввода и можете внести необходимые изменения в данные, которые находятся в этой ячейке.

Вы можете восстановить содержимое ячейки не выходя из режима ввода. Для этого нужно нажать Ctrl+Z. Восстановление данных и выход из режима ввода осуществляется нажатием мышью на красном крестике, расположенном в строке ввода.

При вводе данных почти всегда сталкиваются с проблемой вставки пустой строки или пустого столбца в таблицу. В Excel эта проблема решается следующим образом:

Нажмите мышью на заголовке столбца, перед которым вы собираетесь вставить пустой столбец, в результате чего он будет выделен цветом.

Нажмите правую кнопку мыши. Появится список команд.

Выберите команду Добавить. Появится новый столбец.

Можно вставить столбец и другим способом. Установите маркер в какой-нибудь ячейке столбца, перед которым нужно вставить новый столбец и выполните команду Вставка/Столбец. Аналогично для вставки строки выполните команду Вставка/Строка.

Помимо столбцов и строк в таблицу можно вставлять и ячейки. Для этого выполните команду Вставка/Ячейки.

В Excel имеются следующие способы копирования данных, использующие:

метод «Перетащить и Отпустить»;

команду «Копировать и Вставить»;

средство «Автозаполнение».

При использовании метода «Перетащить и Опустить», а также команд «Вырезать», «Копировать» и «Вставить», Microsoft Excel полностью копирует ячейку, включая формулы и возвращаемые ими значения, примечания и форматы. Если область копирования содержит скрытые ячейки, они также будут скопированы.

ФОРМАТИРОВАНИЕ ДАННЫХ. Данные в Excel выводятся на экран в определенном формате. По умолчанию информация выводиться в формате Общий. Любая последовательность введенных в ячейку символов, которая не может быть интерпретирована Excel как число, формула, дата, время дня, логическое значение или значение ошибки, интерпретируется как текст. Введенный текст автоматически выравнивается в ячейке по левому краю.

С помощью команды <Формат/Формат ячеек> панели Форматирование инструментов ОНЖОМ изменять шрифт, размер символов, стиль и цвет содержимого выделенной ячейки или диапазона. Можно выделить в ячейке отдельный символ и присвоить ему индивидуальный формат. Стиль представляет собой комбинацию форматов, которые можно одновременно применять к выделенному диапазону. В Excel к числам применяют денежный стиль, процентный или с разделением групп разрядов. Можно создавать собственные стили для шрифтов, их размера, числовых форматов, рамок и затенения ячеек, а также защиты ячеек от изменения.

Для форматирования расположения текста в ячейке используется закладка Выравнивание в диалоговом окне <Формат ячеек>.

Здесь можно задать расположение текста для чтения снизу-вверх, сверху-вниз, выровнять по правому, левому, нижнему или верхнему краю ячейки, можно переносить слова текста в пределах ячейки.

С помощью остальных закладок Вы можете отформатировать шрифт, параметры рамки вокруг ячейки, способы заливки ячейки различным цветом, включить или снять защиту с ячейки.

Можно изменить формат представления информации в выделенных ячейках. Для этого выполните команду Ячейки меню Формат. Появится окно диалога <Формат ячеек>, в котором нужно выбрать вкладку Число.

В левой части окна диалога <Формат ячеек> в списке <Числовые форматы> приведены названия всех используемых в Excel форматов .Для формата каждой категории приводится список его шаблонов. При выделении из списка <Числовые форматы> строки <Все форматы> в правом окне Тип отображаются все форматные коды, которые используются для представления на экране информации.

#### ВЫЧИСЛЕНИЯ В ТАБЛИЦАХ

Внесение новых данных в ячейки приводит к автоматическому пересчету всех формул. Если открытые листы содержат большое количество формул, которые требуют много времени на автоматический пересчет, то можно сократить временные затраты. Чтобы отменить автоматический пересчет после каждого внесения изменений в таблицу, выберите команду Параметры в меню Сервис, а затем откройте вкладку Вычисления.

В группе Вычисления можно установить переключатель в одно из положений:

автоматически — обеспечивает вычисление значений формул при каждом внесении изменений в данные, формулу или название. Эта установка используется по умолчанию;

автоматически кроме таблиц — обеспечивает вычисление всех зависящих формул, за исключением таблиц данных. Пересчет таблиц данных будет производиться только при нажатии кнопки Вычислить, отображенной на вкладке, или клавиши F9;

вручную — выполнение вычислений на всех открытых листах будет производиться после нажатия кнопки *Вычислить*, отображенной на вкладке Вычисления или клавиши F9. Для выполнения расчетов только на активном листе нажмите клавиши SHIFT + F9. После установки переключателя в это положение Excel автоматически устанавливает флажок <Пересчет перед сохранением> с тем, чтобы обеспечить сохранение и учет всех введенных данных.

ИСПОЛЬЗОВАНИЕ ФУНКЦИЙ. Excel содержит обширный список стандартных функций, призванных облегчить выполнение простых и сложных вычислений.

Например, функция КОРЕНЬ используется для вычисления положительного значения квадратного корня. Все функции имеют одинаковый формат записи, который включает имя функции и перечень аргументов. Аргументы располагаются в последовательности, определяемой синтаксисом функции, и разделяются запятой.

Запись функции начинается с указания ее имени, затем следует открывающаяся скобка, аргументы и закрывающая скобка. Функция может не иметь аргументов. Она может вводиться в ячейку листа как часть формулы. Функция позволяет выполнить вычисления на листах книги и на листах макросов.

Функции, являющиеся аргументом другой функции, называются вложенными. В формулах Excel можно использовать до семи уровней вложения функций. При неправильной записи формулы на экране может появиться сообщение о циклической ссылке. Имена функций можно набирать строчными буквами. Они будут преобразованы в прописные после нажатия клавиши Enter.

Для вставки функции нажмите кнопку <Вставка функции>, на экране отобразится <Панель формул>. Панель формул появляется также при нажатии кнопки <Вставка функции> на панели инструментов Стандартная.

СРЕДСТВА СТАТИСТИЧЕСКОГО АНАЛИЗА ДАННЫХ. В состав Microsoft Excel входит пакет анализа, предназначенный для решения сложных статистических и инженерных задач. Средства, которые включены в пакет анализа данных, доступны через команду <Анализ данных> в меню Сервис. Если этой команды нет в меню, необходимо загрузить надстройку <Пакет анализа>.

Средства анализа данных позволяют выполнять несколько видов дисперсионного анализа, корреляционный и ковариационный анализ, создавать одномерный статистический отчет, содержащего информацию о центральной тенденции и изменчивости входных данных, производить выборку из генеральной совокупности и т.д.

# ВОПРОС 8. РАБОТА С ТАБЛИЦАМИ КАК С БАЗОЙ ДАННЫХ

СВОДНАЯ ТАБЛИЦА. Сводная таблица призвана помочь пользователю в интерактивном режиме упорядочить и обобщить большое количество данных, приведенных в списках, таблицах и в базах данных. Просмотр больших таблиц требует значительных затрат времени. Сводные таблицы планируются так, чтобы наглядно отобразить интересующую пользователя информацию. На их основе можно создать диаграмму, которая будет отображать все произошедшие изменения.

Если обычные таблицы могут быть только двумерными, то сводные таблицы многомерны, что позволяет избежать дублирования данных. Создавая сводную таблицу, пользователь указывает, какие Поля и какие элементы должны быть представлены в ней. Например, если у вас есть списки товаров, которые продаются в различных магазинах, то названия товаров будут образовывать поля, а их конкретное количество в каждом магазине — элементы. Данные по магазинам, которые расположены в разных городах, можно расположить на отдельных листах. Сводная таблица поможет вам проанализировать суммарную продажу конкретных товаров по неделям, месяцам, кварталам, избавит от необходимости просматривать все имеющиеся списки. В сводную таблицу можно включать промежуточные и итоговые суммы, расчетные поля.

Новые данные вносятся в исходные таблицы, а сводные таблицы предназначены только для чтения. После создания отчета сводной таблицы ее структуру можно изменить, перетаскивая поля и элементы с помощью мыши. Сводная таблица позволяет обобщить и проанализировать данные, которые находятся во внешних источниках данных, созданных без использования Excel. Для более наглядного отображения данных, содержащихся в сводной таблице, можно на их основе создать диаграмму. При создании сводной таблицы можно использовать базу данных, например, таблицу, созданную в Access.

СОЗДАНИЕ СВОДНОЙ ТАБЛИЦЫ. Создание сводной таблицы желательно начать с выделения ячейки внутри используемого списка (это позволяет автоматически выделить диапазон, содержащий исходные данные).

Положением переключателя в группе «Создать таблицу на основе данных, находящихся» установите переключатель в положение: «в

нескольких диапазонах консолидации>, так как источники данных для создания сводной таблицы, расположены на разных листе Excel.

Назначение других положений переключателя:

<в списке или базе данных Microsoft Office Excel> — позволяет создать отчет сводной таблицы или сводной диаграммы по данным строк или столбцов с подписями, расположенных на одном листе Excel;

<во внешнем источнике данных> — позволяет создать отчет сводной таблицы или сводной диаграммы по данным внешнего файла или базы данных, например, Microsoft Access, SQL Server, Paradox.

<в нескольких диапазонах консолидации> — позволяет создать отчет сводной таблицы или сводной диаграммы по данным строк или столбцов с подписями, расположенных в нескольких диапазонах консолидации;

<в другой сводной таблице или сводной диаграмме> — используется для создания отчета сводной таблицы или сводной диаграммы по данным другого отчета сводной таблицы в активной книге.

Со сводными таблицами можно выполнять разнообразные операции — поиск, сортировку, фильтрацию данных в соответствии с критериями, подведение итогов, анализ данных, которые будут изучаться на практических занятиях.

# ТЕМА 3. КОМПЬЮТЕРНЫЕ СЕТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ.

#### СОДЕРЖАНИЕ:

- 1. Назначение и особенности информационно-вычислительных сетей, виды, классификация, топология.
- 2. Характеристика основных видов услуг, предоставляемых сетью Интернет.

ВОПРОС 1. НАЗНАЧЕНИЕ И ОСОБЕННОСТИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ, ВИДЫ, КЛАССИФИКАЦИЯ, ТОПОЛОГИЯ

### 1.1. НАЗНАЧЕНИЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Компьютерные вычислительные сети — принципиально новый вид связи и информационного сервиса, превращающий наше общество в единое информационное пространство, позволяющий одновременно сотням тысяч пользователей совместно решать общие задачи, каждому человеку пользоваться результатами труда всего мирового сообщества, общаться, не придавая значения расстоянию и государственным границам.

Общедоступное информационное взаимодействие называют *телекоммуникацией*, одним из видов которой являются вычислительные (компьютерные) сети.

# 1.2. ОСНОВНЫЕ ПОНЯТИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

В Приказе МВД Республики Беларусь № 1 от 04 января 2010 года понятие Вычислительная сеть подразделения ОВД определяется как информационная сеть, объединяющая средства автоматизации и телекоммуникации одного подразделения ОВД (воинской части) и имеющая выделенное подмножество IP-адресов.

Компьютерная сеть (вычислительная сеть, сеть передачи данных) — единый комплекс, включающий территориально рассредоточенную

систему ЭВМ (компьютеров) и их терминалов, объединенных средствами связи с использованием коммутационного оборудования, программного обеспечения и протоколов для решения информационных, управленческих, вычислительных и других задач.

Сетевая технология — это согласованный набор программных и аппаратных средств — драйверов, сетевых адаптеров, кабелей и разъемов, а также механизмов передачи данных по линиям связи, достаточный для построения вычислительной сети.

Основная цель использования вычислительной сети — обеспечение пользователям сети потенциальную возможность совместного использования ресурсов всех компьютеров.

Для *передачи информации* могут быть использованы различные физические явления:

- электрические сигналы;
- световые сигналы;
- электромагнитное излучение.

Исторически главной целью объединения компьютеров в сеть было разделение ресурсов: пользователи компьютеров, подключенных к сети, или приложения, выполняемые на этих компьютерах, получают возможность автоматического доступа к разнообразным ресурсам остальных компьютеров сети, к числу которых относятся:

- периферийные устройства диски, принтеры, плоттеры, сканеры и др.;
- данные, хранящиеся в оперативной памяти или на внешних запоминающих устройствах;
- вычислительная мощность (за счет удаленного запуска «своих» программ на «чужих» компьютерах).

Сегмент сети — логически или физически обособленная часть сети. Разбиение сети на сегменты осуществляется с целью оптимизации сетевого трафика и повышения безопасности сети в целом.

Для организации компьютерной сети необходимо коммуникационное (сетевое) оборудование.

Сетевое оборудование — устройства, необходимые для работы компьютерной сети — сетевая плата, коммутатор, концентратор, сетевой мост, повторитель, маршрутизатор и др. Обычно выделяют активное и пассивное сетевое оборудование.

Сетевая плата, или сетевая карта, или сетевой адаптер, или Ethernet-адаптер, или NIC (англ. network interface card) — периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети.

Сетевой коммутатор, или свиту (жарг. от англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента.

Сетевой концентратор, или хаб (жарг. от англ. hub — центр деятельности) — сетевое устройство, предназначенное для объединения нескольких устройств Ethernet в общий сегмент сети.

Устройства подключаются при помощи *витой пары*, *коаксиального кабеля* или *оптоволокна*. Термин концентратор (хаб) применим также к другим технологиям передачи данных: USB, FireWire и пр.

В настоящее время хабы почти не выпускаются — им на смену пришли сетевые коммутаторы (свитчи), выделяющие каждое подключённое устройство в отдельный сегмент.

Сетевой мост, или бридж (калька с англ. Bridge) — сетевое оборудование для объединения сегментов локальной сети.

В общем случае коммутатор (свитч) и мост аналогичны по функциональности; разница заключается во внутреннем устройстве: мосты обрабатывают IP-пакеты, используя центральный процессор, коммутатор же использует коммутационную матрицу (аппаратную схему для коммутации пакетов).

Повторитель, или *репитер* (жарг. От англ. repeater) — сетевое оборудование предназначенное для увеличения расстояния сетевого соединения путём повторения электрического сигнала «один в один». Бывают однопортовые и многопортовые повторители. Одной из первых задач, которая стоит перед любой технологией транспортировки данных, является возможность их передачи на максимально большое расстояние.

Маршрутизатор, или роутер, рутер (от англ. Router) — сетевое устройство, на основании информации о топологии сети и определённых правил принимающее решения о пересылке пакетов сетевого уровня между различными сегментами сети.

Функционирование пакетной передачи данных в сети основано на следующем принципе:

- каждая из машин, включенных в сеть, имеет свой собственный номер (идентификатор);
- информация от конкретной ЭВМ поступает в сеть в виде отдельных пакетов;
- пакет всегда имеет информацию о том, для какой машины он предназначен, и свободно перемещается по сети;
- часть пакета с адресом сравнивается с идентификатором каждой ЭВМ и в случае совпадения сообщение принимается;
- если пакет так и не нашел адресата, то через определенное время он уничтожается.

Следует сказать, что рассылка данных и сообщений по сети возможна одновременно для всех ее пользователей: можно, например, послать сообщение не одному конкретному пользователю, а целой группе или всем пользователям сети сразу (в том числе и себе самому). Эта функция сети называется «широковещание».

# 1.3. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

По назначению компьютерные сети разделяются на:

- вычислительные сети, предназначенные главным образом для решения заданий пользователей с обменом данными между их абонентами;
- информационные сети, ориентированные в основном на предоставление информационных услуг пользователям;
- смешанные (информационно-вычислительные), совмещающие функции первых двух.

Для классификации компьютерных сетей используются разные признаки, выбор которых заключается в том, чтобы выделить из существующего многообразия такие, которые позволили бы обеспечить данной классификационной схеме такие обязательные качества:

- возможность классификации всех, как существующих, так и перспективных, компьютерных сетей;
  - дифференциацию существенно разных сетей;
  - однозначность классификации любой компьютерной сети;
- наглядность, простоту и практическую целесообразность классификационной схемы.

В основном компьютерные сети классифицируют по признакам структурной и функциональной организации.

*По территориальной распространенности* сети разделяются на локальные і глобальные.

Покальная сеть LAN (Local Area Network) может описывать и маленькую офисную сеть, и сеть уровня большого завода, занимающего несколько сотен гектаров. Зарубежные источники дают даже близкую оценку — около шести миль (10 км) в радиусе. Локальные сети являются сетями закрытого типа, доступ к ним разрешен только ограниченному кругу пользователей, для которых работа в такой сети непосредственно связана с их профессиональной деятельностью.

Глобальная сеть WAN (Wide Area Network) покрывает большие географические регионы, включает в себя как локальные сети, так и прочие телекоммуникационные сети и устройства. Глобальные сети являются открытыми и ориентированы на обслуживание любых пользователей.

Термин «корпоративная сеть» также используется в литературе для обозначения объединения нескольких сетей, каждая из которых может быть построена на различных технических, программных и информационных принципах.

В учебниках упоминается о так называемых «городских сетях», или сетях мегаполиса (Metropolitan Area Network, MAN). Эти сети предназначены для обслуживания территории крупного города — мегаполиса, и сочетают в себе признаки как локальных, так и глобальных сетей. Появление таких сетей не привело к возникновению каких-нибудь качественно новых технологий, поэтому мы не будем выделять их в отдельный технологический тип сетей.

В соответствии с технологическими признаками, обусловленными средой передачи, компьютерные сети подразделяют на:

- проводные сети, то есть сети, каналы связи которых построены с использованием медных или оптических кабелей;
- *беспроводные сети*, то есть сети, в которых для связи используются беспроводные каналы связи, например радио, СВЧ, инфракрасные или лазерные каналы.

Тип среды передачи влияет на технологию компьютерной сети, так как её протоколы должны учитывать скорость и надежность соединения, обеспечиваемого каналом, а также частоту искажения в нем битов информации. Различие технологий локальных и глобальных сетей во

многом определялось различием качества используемых в этих сетях каналов связи. Качество канала связи зависит от многих факторов, но наиболее кардинально на него влияет выбор проводной или беспроводной среды.

По типу функционального взаимодействия сеть может быть построена по одной из трех схем:

- сеть на основе одноранговых узлов одноранговая сеть;
- сеть на основе клиентов и серверов сеть с выделенными серверами;
- сеть, включающая узлы всех типов гибридная сеть.

Каждая из этих схем имеет свои достоинства и недостатки, определяющие их области применения.

В одноранговых сетях все компьютеры равны в возможностях доступа к ресурсам друг друга. Каждый пользователь может по своему желанию объявить какой-либо ресурс своего компьютера разделяемым, после чего другие пользователи могут с ним работать. В одноранговых сетях на всех компьютерах устанавливается такая операционная система, которая предоставляет всем компьютерам в сети потенциально равные возможности. Сетевые операционные системы такого типа называются одноранговыми ОС.

Изменение роли компьютера в одноранговой сети достигается за счет того, что функции серверной или клиентской частей просто не используются.

Одноранговые сети проще в развертывании и эксплуатации; по этой схеме организуется работа в небольших сетях, в которых количество компьютеров не превышает 10—20. В этом случае нет необходимости в применении централизованных средств администрирования — нескольким пользователям нетрудно договориться между собой о перечне разделяемых ресурсов и паролях доступа к ним.

Однако в больших сетях средства централизованного администрирования, хранения и обработки данных, а особенно защиты данных необходимы. Такие возможности легче обеспечить в сетях с выделенными серверами.

*Клиент-сервер* — вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между

поставщиками услуг (сервисов), называемых *серверами*, и заказчиками услуг, называемых *клиентами*.

Нередко клиенты и серверы взаимодействуют через компьютерную сеть и могут быть как различными физическими устройствами, так и программным обеспечением.

Также термином «рабочая станция» (клиент) обозначают компьютер в составе локальной вычислительной сети (ЛВС) по отношению к серверу.

Компьютеры в локальной сети подразделяются на:

- рабочие станции;
- серверы.

На рабочих станциях пользователи решают прикладные задачи (работают в базах данных, создают документы, делают расчеты). Сервер обслуживает сеть и предоставляет собственные ресурсы всей сети.

*Клиент* — это аппаратный или программный компонент вычислительной системы, посылающий запросы серверу.

Сервер — выделенный компьютер в сети, управляющий сетью или содержащий совместные ресурсы.

Наиболее часто используются следующие виды серверов:

- файловый сервер компьютер, хранящий и обеспечивающий доступ к данным пользователей сети (используются жесткие диски большой емкости или другие типы накопителей);
- сервер баз данных компьютер, выполняющий функции хранения, обработки и управления файлами баз данных;
- *сервер прикладных программ* компьютер, который используется для выполнения прикладных программ на стороне сервера и передачи данных на компьютер клиента.

В больших сетях наряду с отношениями клиент-сервер сохраняется необходимость и в одноранговых связях, поэтому такие сети чаще всего строятся по гибридной (смешанной)схеме.

# 1.4. ТОПОЛОГИЯ ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Сетевая топология (от греч.  $\tau \acute{o}\pi o \varsigma$ , — место) — способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

#### Сетевая топология может быть:

- физической описывает реальное расположение и связи между узлами сети;
- логической описывает движение сигнала в рамках физической топологии;
- информационной описывает направление потоков информации, передаваемых по сети;
- топологией управления обменом это принцип передачи права на пользование сетью.

Мы рассмотрим в рамках классификации физическую топологию сети.

Полносвязная топология — топология компьютерной сети, в которой каждая рабочая станция подключена ко всем остальным. Этот вариант является громоздким и неэффективным, несмотря на свою логическую простоту. Для каждой пары должна быть выделена независимая линия, каждый компьютер должен иметь столько коммуникационных портов сколько компьютеров в сети. По этим причинам сеть может иметь только сравнительно небольшие конечные размеры. Чаще всего эта топология используется в многомашинных комплексах или глобальных сетях при малом количестве рабочих станций.

Ячеистая топология — базовая полносвязная топология компьютерной сети, в которой каждая рабочая станция сети соединяется со всеми другими рабочими станциями этой же сети. Характеризуется высокой отказоустойчивостью, сложностью настройки и преизбыточным расходом кабеля. Каждый компьютер имеет множество возможных путей соединения с другими компьютерами. Обрыв кабеля не приведёт к потере соединения между двумя компьютерами.

Кольцо — базовая топология компьютерной сети, в которой рабочие станции подключены последовательно друг к другу, образуя замкнутую сеть. Наиболее широкое применение получила в оптоволоконных сетях. Используется в стандартах FDDI, Token ring.

Топология типа «шина» представляет собой общий кабель (называемый шина или магистраль), к которому подсоединены все рабочие станции. На концах кабеля находятся терминаторы, для предотвращения отражения сигнала.

Звезда — базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно сетевой концентратор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии (как правило «дерево»).

Иногда имеет смысл строить сеть с использованием нескольких концентраторов, иерархически соединенных между собой связями типа «звезда». Получаемую В результате структуру называют также «деревом». В настоящее время дерево является самым распространенным типом топологии связей, как в локальных, так и в глобальных сетях.

Смешанная топология — топология, преобладающая в крупных сетях с произвольными связями между компьютерами. В таких сетях можно выделить отдельные произвольно связанные фрагменты (подсети), имеющие типовою топологию, поэтому их называют сетями со смешаной топологией.

До конца XX века основными каналами распространения информации были каналы передачи аудио- и видеосигналов. В 80-е годы XX века произошёл скачёк в развитии глобальных информационных и коммуникационных технологий. Появился третий канал распространения информации, который коренным образом повлиял на развитие системы средств массовой информации. После радио- и телевещания были изобретены сетевые технологии, основанные на ином, цифровом, способе передачи информации, которые привели к формированию новой среды для распространения потоков информации.

Быстрое развитие компьютерных технологий, и компьютерных сетей в частности, существенно возможности для доступа к информации различного рода и для общения людей. Информация, имеющаяся в Интернете более динамична, чем в печатных книжных изданиях. В Интернете легче внести некоторые изменения, так как не надо перепечатывать весь текст. Благодаря Интернету можно получить более

свежую информацию об изменениях в законодательстве и других правовых документах. В Республике Беларусь создан Национальный правовой Интернет-портал, предоставляющий правовую информацию пользователям Интернета. Поскольку юристу в своей работе приходится пользоваться документами законодательного характера, то ему необходимо уметь пользоваться Интернетом и искать достоверную правовую информацию.

#### 1.5. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

Для конечного пользователя сеть — это не компьютеры, кабели и концентраторы и даже не информационные потоки, для него сеть — это, прежде всего, набор сетевых служб, с помощью которых он получает возможность просмотреть список имеющихся в сети компьютеров, прочитать удаленный файл, распечатать документ на «чужом» принтере почтовое сообшение. Именно послать совокупность ИЛИ предоставляемых возможностей — насколько широк ИХ выбор, насколько они удобны, надежны и безопасны — определяет для пользователя облик той или иной сети.

Сетевые программные средства — это программное обеспечение, предназначенное для управления работой информационной сети и обеспечения пользовательского интерфейса.

К сетевым программным средствам относятся:

- сетевая операционная система;
- сетевые приложения.

Сетевая операционная система — операционная система со встроенными возможностями для работы в компьютерных сетях.

Главными задачами являются разделение ресурсов сети (например, дисковые пространства) и администрирование сети. С помощью сетевых функций системный администратор определяет разделяемые ресурсы, задаёт пароли, определяет права доступа для каждого пользователя или группы пользователей. Это порождает разделение ОС на:

- сетевые ОС для серверов;
- сетевые ОС для пользователей.

К таким возможностям можно отнести:

- поддержку сетевого оборудования;
- поддержку сетевых протоколов;

- поддержку протоколов маршрутизации;
- поддержку фильтрации сетевого трафика;
- поддержку доступа к удалённым ресурсам, таким как принтеры, диски и т. п. по сети;
- поддержку сетевых протоколов авторизации;
- наличие в системе сетевых служб, позволяющих удалённым пользователям использовать ресурсы компьютера.

Кроме собственно обмена данными, сетевые службы должны решать и другие, более специфические задачи, например, задачи, связанные с распределенной обработкой данных. К таким задачам относятся:

- обеспечение непротиворечивости нескольких копий данных, размещенных на разных машинах (служба репликации);
- организация выполнения одной задачи параллельно на нескольких машинах сети (служба вызова удаленных процедур).

Среди сетевых служб можно выделить административные, то есть такие, которые в основном ориентированы не на простого пользователя, а на администратора, и служат для обеспечения правильной работы сети в целом.

Реализация сетевых служб осуществляется программными средствами. Все сетевые службы построены в архитектуре «клиент-сервер», которую мы рассматривали выше.

Сетевой операционной системой предоставляются основные службы:

- файловая служба;
- веб-служба;
- служба печати.

Вспомогательные службы предоставляются системными сетевыми приложениями или утилитами, работающими в тесном контакте с сетевой операционной системой:

- служба баз данных;
- факсимильной связи;
- передачи голоса и др.

Одним из главных показателей качества сетевой службы является ее удобство. При определении степени удобства разделяемого ресурса часто употребляют термин «прозрачность».

Прозрачный доступ — это такой доступ, при котором пользователь не замечает, где расположен нужный ему ресурс — на его компьютере или на удаленном.

Например, после того как пользователь смонтировал удаленную файловую систему в свое дерево каталогов, доступ к удаленным файлам становится для него совершенно прозрачным.

Примеры сетевых операционных систем:

- Novell NetWare;
- Microsoft Windows (95, NT, XP, Vista и Seven);
- различные UNIX системы, такие как Solaris, FreeBSD;
- различные GNU/Linux системы.

К сетевым приложениям относятся:

- электронная почта обеспечивает доставку писем (а часто и произвольных файлов, а также голосовых и факсимильных сообщений) от одних пользователей локальной сети другим, а иногда позволяет общаться и с удаленными пользователями по модему или через InterNet;
- средства удаленного доступа позволяют подключаться к локальной сети с помощью модема и работать на компьютере, как будто он непосредственно подключен в сеть (разумеется, при этом многие операции будут выполняться дольше, так как модем работает значительно медленнее сетевого контроллера);
- средства групповой работы (наиболее популярно из них Lotus Notes) позволяют совместно работать над документами, обеспечивают согласованность версий документов у разных пользователей, документооборота предоставляют средства организации ДЛЯ телеконференции организовывать позволяют предприятия, письменный обмен мнениями по различным темам и т.д.;
- программы резервирования позволяют создавать резервные копии данных, хранящихся на серверах локальной сети и на компьютерах пользователей, а при необходимости восстанавливать данные по их резервной копии;
- средства управления вычислительной сетью позволяют управлять ресурсами вычислительной сети с одного рабочего места, получать информацию о состоянии и загрузке сети, настраивать производительность сети, управлять системами пользователей сети (например, устанавливать на них программное обеспечение) и т.д.

#### ВЫВОД ПО ВОПРОСУ:

# ВОПРОС 2. ХАРАКТЕРИСТИКА ОСНОВНЫХ ВИДОВ УСЛУГ, ПРЕДОСТАВЛЯЕМЫХ СЕТЬЮ ИНТЕРНЕТ

В дословном переводе на русский язык Интернет — это межсеть, то есть в узком смысле слова ИНТЕРНЕТ — это объединение сетей. Однако в последние годы у этого слова появился и более широкий смысл — Всемирная компьютерная сеть. Интернет можно рассматривать в физическом смысле как миллионы компьютеров, связанных друг с другом всевозможными линиями связи, однако такой «физический» взгляд на Интернет слишком узок. Лучше рассматривать Интернет как некое информационное пространство.

#### 2.1. ЮРИДИЧЕСКИЕ АСПЕКТЫ

Интернет как явление имеет особенностей юридического характера:

- у Интернета нет собственника, так как он является совокупностью сетей, которые имеют различную географическую принадлежность;
- Интернет нельзя выключить целиком, поскольку маршрутизаторы сетей не имеют единого внешнего управления;
- Интернет стал достоянием всего человечества;
- у Интернета имеется много полезных и вредных свойств, эксплуатируемых заинтересованными лицами;
- Интернет, прежде всего, средство открытого хранения и распространения информации. По маршруту транспортировки незашифрованная информация может быть перехвачена и прочитана;
- Интернет может связать каждый компьютер с любым другим, подключённым к Сети, так же, как и телефонная сеть. Если телефон имеет автоответчик, он способен распространять информацию, записанную в него, любому позвонившему;
- сайты в Интернете распространяют информацию по такому же принципу, то есть индивидуально, по инициативе читателя;
- спам-серверы и «зомби-сети» распространяют информацию по инициативе отправителя и забивают почтовые ящики пользователей электронной почты спамом точно так же, как забивают реальные почтовые ящики распространители рекламных листовок и брошюр.

Распространение информации в Интернете имеет такую же природу, как и слухи в социальной среде. Если к информации есть большой интерес, она распространяется широко и быстро, нет интереса — нет распространения.

Чтение информации, полученной из Интернета или любой другой сети ЭВМ, относится, как правило, к непубличному воспроизведению произведения. За распространение информации в Интернете (разглашение), если это государственная или иная тайна, клевета, другие запрещённые законом к распространению сведения, вполне возможна юридическая ответственность по законам того места, откуда информация введена.

#### 2.2. СПОСОБЫ ПОДКЛЮЧЕНИЯ К ИНТЕРНЕТУ

Самыми распространенными способами подключения к Интернету на сегодняшний день являются:

- модемное соединение (Коммутируемый доступ) Dial-Up или ADSL;
- GPRS доступ (через сотовый телефон);
- соединение по выделенной линии (оптоволокно и т.д.);
- подключение через кабельное телевидение;
- радиодоступ;
- подключение через CDMA или GSM модем.
- спутниковое соединение.

Все они отличаются друг от друга принципом работы, скоростью передачи данных, надежностью, сложностью настройки оборудования и ценой. Основная характеристика любого подключения к Интернету — скорость передачи данных — измеряется в количестве информации передаваемой пользователю за единицу времени (за одну секунду) и обычно измеряется в килобайтах/сек (КВ/s) или килобитах/сек (kbps). Для высокоскоростных каналов измерение скорости уже идет в мегабитах или мегабайтах в секунду.

В принципе времяпрепровождение в Интернете можно разделить на две группы — требующее получение большого количества трафика и не требующее этого. Для веб-серфинга (просмотра страниц) достаточно

скорости обычного модемного соединения. Однако такая скорость не позволит вам комфортабельно скачивать большие файлы — фильмы, качественную музыку и так далее. Поэтому для полноценного использования возможностей Интернета требуется высокоскоростной доступ.

Модемное соединение (dial-up) — самый старый, но всё ещё широко используемый способ подключения. Модемное (dial-up) подключение сейчас используется только там, где есть операторы абонентской телефонной связи, предоставляющие услуги dial-up подключения, и нет других способов подключения. Для подключения этим способом необходимо наличие dial-up модема и стационарного телефона. У этого способа подключения плюсы такие: это сама возможность подключения к интернету, низкая стоимость модема, простота настройки и установки. А вот минусов гораздо больше — низкая скорость передачи данных, если Вы подключились к интернету, то к вам уже никто не дозвонится — телефон будет занят, платить надо как за интернет, так и за телефон, скачать большие файлы практически невозможно из-за низкого качества передачи данных, да и дорого.

*ADSL* — более современный способ подключения к интернету. Тут также как и при Dial-Up подключении, необходимо наличие модема, правда уже цифрового ADSL (Asymmetric Digital Subscriber Line), и стационарного телефона. Кроме того, на вашем компьютере должна быть установлена сетевая карта.

Минус этого способа подключения — это высокая стоимость подключения. Зато плюсов больше — качественная, высокая скорость передачи данных, телефон не занят, даже если у вас блокиратор, возможность подключиться к безлимитному пакету.

*GPRS-соединение* — подключение через мобильный телефон. В связи с быстрым развитием сотовой связи, почти у каждого человека имеется сотовый телефон, поэтому именно этот способ подключения становится всё более популярным. Для подключения этим способом к интернету необходимо наличие мобильного телефона с поддержкой GPRS или EDG протоколов (любой современный, не старше 2х-3х лет, мобильный телефон поддерживает эти протоколы) и средства связи с компьютером — USB кабель, Bluetooth, инфракрасный порт.

Неоспоримый плюс данного способа — это мобильность. Скорость и качество передачи данных зависит от средства подключения к компьютеру и протокола связи, и в целом достаточно приемлемые. Минус данного подключение конечно стоимость, к сожалению, она всё ещё высокая.

Соединение по выделенной линии — Сейчас многие провайдеры<sup>3</sup> предоставляют услуги подключения к интернету через выделенную линию. Без углубления в технические подробности можно сказать, что выделенная линия — это линия связи, канал передачи данных. При таком подключении передача данных осуществляется с помощью специального кабеля (оптоволокно или витая пара), который с одной стороны подключен к оборудованию провайдера, обычно расположенное в подвале или на чердаке здания, а с другой стороны в сетевую карту вашего компьютера. Передача данных может осуществляться беспроводно, с помощью WiFi соединения, что очень удобно при перемещении в пределах здания. У этого способа подключения только плюсы, это и высокая, очень качественная передача данных, и невысокая подключения безлимитного И возможность мобильность при WiFi соединении. Единственное, что необходимо — это наличие сетевой карты и если есть WiFi, то нужен WiFi адаптер.

Подключение через кабельное телевидение — подключение, при котором используются специальные кабельные модемы. Этот способ может быть интересен в том случае, если у Вас в доме есть оператор кабельного телевидения (если на Вашем телевизоре настроено от тридцати до ста каналов, то оператор кабельного телевидения в вашем доме есть) и нет непосредственно провайдера услуг интернета. Качество и скорость передачи данных на высокам уровне, цены на услуги не высокие. Правда, сам модем немного дороговат, но некоторые операторы предлагают модемы в аренду с последующим выкупом.

Радиодоступ используется в том случае, если провайдер по какимлибо причинам не может протянуть кабель желаемое место использования интернета, но может предоставить беспроводную точку Точка доступа должна находиться В пределах прямой видимости, на расстоянии не более 5 км от желаемого места интернета. Если использования все условия выполнены, ОНЖОМ

 $<sup>^{3}</sup>$  Провайдер это фирма, которая предоставляет услугу подключения к интернету.

устанавливать специальную антенну, точно так же как бы ставили телевизионную (на крыше, столбе, дереве) и направить рупор антенны непосредственно на точку доступа. Сама антенна подключается кабелем к радиокарте на компьютере. Качество и скорость передачи данных приемлемые, правда, могут зависеть от погодных условий. На оборудование конечно надо будет потратиться.

Подключение через CDMA или GSM модем имеет такое преимущество, как мобильность и независимость от мобильного телефона. Любой CDMA или GSM оператор предоставляет услуги интернета, у него же Вы сможете купить модем. Характеристики скорости и качества передачи данных такие же как и при подключении через мобильный телефон.

Спутниковое соединение. Ещё совсем недавно такой способ подключения был практически не доступен для обычных пользователей. Сейчас же ситуация меняется. Количество провайдеров, предоставляющих услуги подключения спутникового интернета, увеличивается с каждым днём и как следствие падают цены на услуги. Спутниковый интернет используется, когда нет другой альтернативы подключения. Вы можете находиться где угодно: в пустыне, глухой тайге, на необитаемом острове — спутниковый интернет у вас будет! Спутниковый интернет может быть односторонним (работает только на (прием двухсторонним отправка). И Преимущества спутникового подключения к Интернету — в первую очередь это очень низкая стоимость трафика. Стоимость комплекта оборудования и подключения в настоящее время доступна практически для всех и составляет приблизительно 200-300 долларов США (имеется в виду одностороннее подключение). Скорость передачи данных значительно от провайдера И тарифного варьируется зависимости Провайдеры спутникового Интернета выбранного пользователем. предлагают очень широкий выбор тарифных планов, в том числе и безлимитных. Очень приятным бонусом является также возможность бесплатного приема спутникового телевидения. Минусом одностороннего спутникового подключения к Интернету является необходимость наличия канала для исходящего трафика — телефонной линии или телефона с поддержкой GPRS. Впрочем, сейчас это не такая большая проблема. Минус двухстороннего спутникового подключения высокая цена оборудования. Для подключение спутникового интернета необходимо такое оборудование:

- спутниковая антенна;
- спутниковый модем;
- конвертор для преобразования сигнала.

#### 2.3. УСЛУГИ ИНТЕРНЕТА

Рассмотрим наиболее популярные услуги Интернета.

Всемирная паутина («WWW»World Wide Web) — распределенная предоставляющая между собой система, доступ К связанным документам, расположенным на различных компьютерах, подключенных к Интернету. Всемирную паутину образуют миллионы web-серверов. Большинство ресурсов всемирной паутины представляет собой гипертекст. Гипертекстовые документы, размещаемые всемирной паутине, называются web-страницами. Несколько webстраниц, объединенных общей темой, дизайном, а также связанных между собой ссылками и обычно находящихся на одном и том же webсервере, называются web-сайтом. Для загрузки и просмотра web-страниц используются специальные программы — браузеры. Всемирная паутина вызвала настоящую революцию в информационных технологиях и бум в развитии Интернета. Часто, говоря об Интернете, имеют в виду именно Всемирную паутину, однако важно понимать, что это не одно и то же. Кроме этого можно указать следующие услуги:

- группы новостей;
- файлообменные сети;
- электронные платёжные системы;
- Интернет-радио или веб-радио;
- Интернет-телевидение;
- ІР-телефония;
- мгновенный обмен сообщениями через Интернет;
- FTР-серверы;
- IRC (ретранслируемый интернет-чат);
- поисковые системы;
- Интернет-реклама;
- удалённые терминалы;
- удалённое управление; WEB 2.0;

многопользовательские игры.

#### 2.3.1. Во Всемирной паутине можно выделить:

- веб-форумы;
- блоги;
- вики-проекты;
- Интернет-магазины;
- Интернет-аукционы;
- социальные сети.

*Веб-форумы* — класс веб-приложений для организации общения посетителей веб-сайта. Термин соответствует смыслу исходного понятия «форум».

*Блог* (англ. blog, от «web log», «сетевой журнал или дневник событий») — веб-сайт, основное содержимое которого — регулярно добавляемые записи, содержащие текст, изображения или мультимедиа. Для блогов характерны недлинные записи временной значимости, отсортированные в обратном хронологическом порядке (последняя запись сверху). Отличия блога от традиционного дневника обусловливаются средой: блоги обычно публичны и предполагают сторонних читателей, которые могут вступить в публичную полемику с автором (в комментарии к блогозаписи или своих блогах).

Вики-проект — (англ. wiki) веб-сайт, структуру и содержимое которого пользователи могут сообща изменять с помощью инструментов, предоставляемых самим сайтом. Известнейший вики-сайт — Википедия. Впервые термин «вики» для описания веб-сайта был использован в 1995 году Уордом Каннингемом, разработчиком первой вики-системы WikiWikiWeb, который заимствовал слово гавайского языка, означающее «быстрый».

Интернет-магазин (англ. online shop или e-shop) — веб-сайт, рекламирующий товар или услугу, принимающий заказы на покупку, предлагающий пользователю выбор варианта расчета, способа получения заказа и выписывающий счет на оплату.

Интернет-аукцион (он же «онлайновый аукцион») — аукцион, проводящийся посредством интернета. В отличие от обычных аукционов, интернет-аукционы проводятся на расстоянии (дистанционно) и в них можно участвовать, не находясь в определённом

месте проведения, делая ставки через интернет-сайт или компьютерную программу аукциона.

Социальная сеть направлена на построение сообществ в Интернете из людей со схожими интересами и/или деятельностью. Связь осуществляется посредством сервиса внутренней почты или мгновенного обмена сообщениями.

- 2.3.2. Электронная почта и списки рассылки (англ. email, e-mail, oт англ. electronic mail) технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети. Основным отличием от прочих систем передачи сообщений (например, служб мгновенных сообщений) является возможность отложенной доставки и развитая (и запутанная из-за длительного времени развития) система взаимодействия между независимыми почтовыми серверами.
- 2.3.3. Группы новостей (в основном, Usenet) (англ. newsgroup) (другое название ньюсгруппа или ньюзгруппа) виртуальное вместилище сообщений в технологии NNTP, аналог канала в IRC. Иногда вместо термина группа новостей не вполне грамотно используется конференция. Группы обозначаются названиями, состоящими из слов, разделённых точками (.), например gnu.emacs.help. Термин группа новостей является сугубо техническим и ничего не говорит о принадлежности, назначении или правилах управления новостным ресурсом. Большинство существующих групп новостей принадлежит Usenet.
- **2.3.4.** Файлообменные сети собирательное название сетей для совместного использования файлов. Часто в основе файлообменных сетей лежат одноранговые компьютерные сети, основанные на равноправии участвующих в обмене файлами, то есть каждый участник одновременно является и клиентом, и сервером.

- 2.3.5. Электронные платёжные системы совокупность процедур и связанных с ними компьютерных сетей, используемых для проведения финансовых транзакций на рынке облигаций, валютном рынке, на рынке производных финансовых инструментов и опционов, и для передачи средств между участниками этой платёжной системы.
- **2.3.6. Интернет-радио**, или **веб-радио** группа технологий передачи потоковых аудиоданных через сеть Интернет. Также в качестве термина интернет-радио, или веб-радио, может пониматься радиостанция, использующая для вещания технологию потокового вещания в Интернет.
- 2.3.7. Интернет-телевидение (англ. Internet Protocol Television, сокращённо IPTV) — система, использующая двухсторонний цифровой сигнал радиопередачи, который посылается через переключенную телефонную кабельную сеть ИЛИ посредством широкополосного Оно базируется IP подключения. на декодировании видео преобразовании его в стандартные телевизионные сигналы.
- **2.3.8. IP-телефония** (англ. Voice over IP; IP-телефония) система связи, обеспечивающая передачу речевого сигнала по сети Интернет или по любым другим IP-сетям. Сигнал по каналу связи передаётся в цифровом виде и, как правило, перед передачей преобразовывается (сжимается) с тем, чтобы удалить избыточность.
- **2.3.9. Мгновенный обмен сообщениями через Интернет** (англ. Instant messenger, IM) программа для обмена сообщениями через Интернет в реальном времени через службы мгновенных сообщений (Instant Messaging Service, IMS). Передаваться могут текстовые сообщения, звуковые сигналы, изображения, видео, а также производиться такие действия как совместное рисование или игры. Такая программа может применяться для организации видеоконференций.

- **2.3.10. FTP-серверы** (англ. File Transfer Protocol протокол передачи файлов) протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.
- **2.3.11. IRC** (реализовано также как веб-чаты) (англ. Internet Relay Chat ретранслируемый интернет-чат) сервисная система, при помощи которой можно общаться через сеть Интернет с другими людьми в режиме реального времени. Она была создана в 1988 году финским студентом Ярко Ойкариненом (Jarkko Oikarinen). В русском компьютерном сленге IRC называют «иркой», «ирцем».
- **2.3.11. Поисковые системы** программно-аппаратный комплекс с веб-интерфейсом, предоставляющий возможность поиска информации в Интернете. В просторечии под поисковой системой подразумевают веб-сайт, на которой размещён интерфейс (фронт-энд) системы. Программной частью поисковой системы является поисковая машина (поисковый движок) комплекс программ, обеспечивающий функциональность поисковой системы и являющийся коммерческой компании-разработчика поисковой системы. Большинство поисковых систем ищут информацию на сайтах Всемирной паутины, но существуют также системы, способные искать файлы на ftp-серверах, товары в интернет-магазинах, а также информацию в группах новостей Usenet.
- 2.3.12. Интернет-реклама особый вид рекламы с использованием различных интернет-средств. С интернет-рекламой тесно связано понятие рекламного места. Рекламное место место, выделенное в дизайне рекламной площадки для размещения рекламных материалов определённого типа. Хорошим тоном считается такой дизайн рекламного места, при котором оно явно отделено от основного содержания сайта. Как правило, более дорогими являются рекламные места, попадающие «на первый экран», то есть не требующие для просмотра листания (скроллирования) веб-страницы.

- 2.3.13. Удалённые терминалы служба удаленного управления компьютером Telnet. Подключившись к удаленному компьютеру по протоколу этой службы, можно управлять его работой. Такое управление еще называют консольным или терминальным. Каждый сервер, предоставляющий Telnet-услуги, обычно предлагает свое клиентское приложение. Его надо получить по сети (например, по протоколу FTP), установить на своем компьютере, подключиться к серверу и работать с удаленным оборудованием.
- **2.3.14.** Удалённое управление (управляемые услуги) практика передачи постоянных видов деятельности менеджмента за пределы организации. Термин является близким по значению к слову «аутсорсинг».
- **2.3.15. Многопользовательские игры** компьютерная игра, в которую одновременно играют несколько человек.
- **2.3.16. WEB 2.0** (определение Тима О'Рейли) методика проектирования систем, которые путём учета сетевых взаимодействий становятся тем лучше, чем больше людей ими пользуются. Особенностью веб 2.0. является принцип привлечения пользователей к наполнению и многократной выверке контента. Определение Тима О'Рейли нуждается в уточнении. Говоря «становятся лучше», имеют в виду скорее «становятся полнее», то есть речь, как правило, идёт о наполнении информацией, однако вопросы её надёжности, достоверности, объективности не рассматриваются.

# 2.4. ПРОТОКОЛЫ И АДРЕСАЦИЯ, ИСПОЛЬЗУЕМЫЕ В ИНТЕРНЕТ

# 2.4.1. Протоколы

В Интернет наиболее распространены:

- протокол ТСР;
- протокол IP.

Образно говоря протокол — это «язык», используемый компьютерами для обмена данными при работе в сети. Чтобы различные компьютеры сети могли взаимодействовать, они должны «разговаривать» на одном «языке», то есть использовать один и тот же протокол.

*Протокол* — это правила передачи данных между узлами компьютерной сети.

Систему протоколов Интернет называют «стеком протоколов TCP/IP».

Протокол TCP — протокол транспортного уровня. Он управляет тем, как происходит передача данных. Согласно протоколу TCP, отправляемые данные «нарезаются» на небольшие пакеты, после чего каждый пакет маркируется таким образом, чтобы в нем были данные, необходимые для правильной сборки документа на компьютере получателя. Когда мы работаем в Интернете, то по одной единственной телефонной линии можем одновременно принимать документы из Америки, Австралии и Европы. Пакеты каждого из документов поступают порознь, с разделением во времени, и по мере поступления собираются в разные документы.

Протокол IP — адресный. Он принадлежит сетевому уровню и определяет, куда происходит передача. Его суть состоит в том, что у каждого участника Всемирной сети должен быть свой уникальный адрес (IP-адрес). Без этого нельзя говорить о точной доставке TCP-пакетов на нужное рабочее место. Этот адрес выражается очень просто — четырьмя байтами, например 195.38.46.11. Каждый компьютер, через который проходит какой-либо TCP-пакет, может по этим четырем числам определить, кому из ближайших «соседей» надо переслать пакет, чтобы он оказался «ближе» к получателю. Поскольку один байт содержит до 256 различных значений, то теоретически с помощью четырех байтов можно выразить более четырех миллиардов уникальных IP адресов. На практике же из-за особенностей адресации к некоторым типам локальных сетей количество возможных адресов составляет порядка двух миллиардов.

## 2.4.2. Адресация объектов в Интернет

Гипертекстовая связь между миллиардами документов, хранящихся на физических серверах Интернета, является основой существования логического пространства World Wide Web. Адрес любого файла во всемирном масштабе определяется унифицированным указателем ресурса — URL.

# Адрес URL состоит из трех частей:

- 1. Указание службы, которая осуществляет доступ к данному ресурсу (обычно обозначается именем прикладного протокола, соответствующего данной службе). Так, например, для службы WWW прикладным является протокол HTTP (Hypertext Transfer Protocol протокол передачи гипертекста). После имени протокола ставится двоеточие (:) и два знака «/» (косая черта): http://...
- 2. Указание доменного имени компьютера (сервера), на котором хранится данный ресурс: http://www.abcde.com...
- 3. Указания полного пути доступа к файлу на данном компьютере. В качестве разделителя используется символ «/» (косая черта): http://www.abcde.com/Files/New/abcdefg.zip.

В Интернете строчные и прописные символы считаются разными. Когда мы говорили о протоколах Интернета, то сказали, что адрес любого компьютера или любой локальной сети в Интернете может быть выражен четырьмя байтами, например, так: 195. 28. 132. 97.

В Интернете этот же адрес может быть задан и в другом виде, например, так: www.abcdef.com.

Это две разных формы записи адреса одного и того же сетевого компьютера. Человеку неудобно работать с числовым представлением IP-адреса, зато доменное имя запоминается легко, особенно если учесть, что, как правило, это имя содержательное. Например, Web-сервер компании Microsoft имеет имя www.microsoft.com, а поисковый Web-сервер белорусского домена — by имеет имя www.tut.by.

С другой стороны, автоматическая работа серверов сети организована с использованием четырехзначного числового адреса. Поэтому необходим перевод доменных имен в связанные с ними IP-адреса. Этим и занимаются серверы службы имен доменов DNS. Наш запрос на получение одной из страниц сервера www.abcde.com сначала

обрабатывается сервером DNS, и далее он направляется по IP-адресу, а не по доменному имени.

# ТЕМА 4. ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

# 1. Информационные угрозы и компьютерные преступления

В современном мире информация становится стратегическим ресурсом, одним из основных богатств экономически развитого государства. Быстрое совершенствование информатизации в стране, проникновение ее во все сферы жизненно важных интересов личности, общества и государства вызвали помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость защиты информации. Учитывая, что в настоящее время экономический потенциал все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная **УЯЗВИМОСТЬ** экономики OTинформационных воздействий.

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, "безбумажного" документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем на сегодняшний день.

# 1.1. Информационные угрозы

Под **угрозой безопасности информации** понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют компьютерным пиратом, или хакером.

В своих противоправных действиях, направленных на овладение найти чужими секретами, взломщики стремятся такие источники конфиденциальной информации, которые наиболее бы давали им достоверную информацию в максимальных объемах с минимальными затратами на ее получение. С помощью различного вида уловок и множества приемов и средств подбираются пути и подходы к таким источникам. В данном случае под источником информации понимается материальный обладающий определенными сведениями, представляющими конкретный интерес для злоумышленников или конкурентов.

Если ценность информации теряется при ее хранении и/или распространении, то реализуется угроза нарушения\_конфиденциальности информации. Если информация изменяется или уничтожается с потерей ее ценности, то реализуется угроза целостности информации. Если информация вовремя не поступает легальному пользователю, то ценность ее уменьшается и со временем полностью обесценивается, тем самым реализуется угроза оперативности использования или доступности информации.

К угрозам нарушения конфиденциальности информации относят хищение (копирование) и утечку информации; к угрозам доступности — блокирование информации; к угрозам целостности — модификацию (искажение информации), отрицание подлинности информации или навязывание ложной информации.

Традиция выделять именно упомянутые три вида угроз безопасности информации относится к принятым в 1983 году «Критериям оценки компьютерных систем Министерства обороны США», более известным как «Оранжевая книга». Данный подход полностью сохранился и в Международном стандарте ИСО/МЭК 15408-99 (исторически сложившееся название — «Общие критерии»), и в его Российском аналоге ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий».

Данные нормативные документы, как следует из их направленности, ориентированы в основном на компьютерные системы обработки информации. Принципиальной особенностью таких систем является то, что в них субъект отстраняется от процесса обработки информации и неявным образом делегирует свои полномочия по отдельным составляющим рассмотренного выше информационного процесса определенной аппаратнопрограммной среде, «которая обладает некоторой свободой в своих действиях и совсем не обязательно делает то, что хочет или предполагает пользователь».

Вместе с тем, в общем случае необходимость «раскладывания» конкретных примеров отрицательного воздействия внешних факторов на информационный процесс некоторого субъекта всего лишь по трем «делам» (конфиденциальность-доступность-целостность) может вызывать значительные проблемы.

И вопрос здесь не столько в необходимости учета особенностей различных источников угроз безопасности (антропогенные — преднамеренные и случайные, техногенные, природные), сколько в трудностях корректной правовой оценки соответствующих явлений.

За противоправные действия виновные лица могут нести гражданско-правовую, административную, уголовную и иную ответственность. При этом наибольшая степень наказания личности нарушителя обеспечивается при наличии уголовных санкций, когда правонарушения в зависимости от их общественной значимости, массовости, типичности и устойчивости проявления переводятся (криминализируются) в разряд преступлений.

К другим негативным явлениям, сопровождающим информационные процессы и вместе с тем вызывающим сложности правовой квалификации, также следует отнести:

незаконную продажу баз данных об абонентах мобильной связи;

незаконную продажу архивов SMS-сообщений;

незаконный доступ к служебной информации о местонахождении абонентов (отслеживание роуминга);

распространение оскорбительных и непристойных материалов в сети Интернет (спамминг);

нарушение прав интеллектуальной собственности;

продажу аппаратно-программных средств с недекларированными возможностями.

Список можно продолжать еще долго.

Классификация угроз информационной безопасности всего лишь из трех составляющих (нарушения конфиденциальности, целостности, доступности) в значительном числе практически важных случаев скорее порождает вопросы, чем помогает отвечать на них.

Действительно, является ли реализацией угрозы информационной безопасности использование чужих сообщений как стеганографических контейнеров для передачи засекреченных сообщений (пусть даже используемых для подготовки преступления), если при этом качество передачи чужого сообщения практически не нарушалось? Насколько общество (законодатель) могут игнорировать нелегальное использование чужой информации как носителя сообщений, содержащих общественно опасную информацию?

Или другое, насколько безобидны действия оператора связи, если в результате перегрузки системы, существующей по его вине, информация до адресата поступает с существенным опозданием?

Казалось бы, такого рода событие является скорее досадным обстоятельством, нежели опасным явлением. Однако следует вспомнить, что

при этом нарушается одно из главных свойств информации — ее своевременность.

Итак, становится очевидным, что существующая классификация угроз информационной безопасности требует своего развития и уточнения. Не случайно в проекте Европейской конвенции о киберпреступности объективная сторона киберпреступлений характеризуется выделением гораздо большего числа групп общественно опасных деяний, то есть гораздо большей детализацией, чем классификация из трех видов. В частности, Европейская конвенция различает противозаконный доступ (статья 2) и противозаконный перехват данных (статья 3), вмешательство в функционирование системы (статья 5) и противоправное использование устройств (статья 6), подлог с использованием компьютеров (статья 7) и мошенничество с использованием компьютеров (статья 8), правонарушения, связанные с содержанием данных (статья 9) и с нарушением авторского права (статья 10).

С точки зрения любой отрасли права (гражданского, административного, уголовного и др.) современные угрозы информационной безопасности не должны быть ограничены известной классификацией, включающей в себя нарушения лишь конфиденциальности, доступности и целостности информации. Новые особенности информационного процесса в современном мире вызывают необходимость обновления содержательного значения термина «угроза информационной безопасности».

При этом является важным и очевидным участие в разработке обновленной классификации угроз информационной безопасности всех заинтересованных специалистов.

# 1.2. Компьютерные преступления

Компьютерная преступность, или преступление с использованием компьютера — представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует.

Укажем основные виды компьютерных преступлений.

Внедрение компьютерного вируса — процесс внедрение вредоносной программы с целью нарушения работы ПК. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Вирус может проявлять себя в разных формах. Это могут быть замедления в

выполнении программ; увеличение объема программных файлов и, наконец, эти проявления могут привести к стиранию файлов и уничтожению программного обеспечения.

Несанкционированный доступ к информации может осуществляться с целью её хищения или же ради развлечения и последующего использования данной информации. Существуют множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения модификацией программного и информационного обеспечения, хищением носителей информации; установкой аппаратуры записи и т.д.

Подделка выходной информации может преследовать различные цели. Итогом подделки является то, что конечному потребителю информации будут предоставлены недостоверные данные. Примером могут служить подтасовка результатов выборов или же хищение различного вида товаров, путем ввода в программу фальшивых данных; подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

Несанкционированное копирование конфиденциальной информации. В процессе неизбежны работы каждой компании случаи конфиденциальной информации. Несмотря на то, что защитные системы, отвечающие за хранение и доступ к внутренней информации, постоянно совершенствуются, проблема продолжает существовать. Организации несут огромные потери несанкционированного распространения из-за конфиденциальной информации. Несанкционированное копирование может осуществляться посредством изъятия средств компьютерной техники; перехвата информации; несанкционированного доступа к технике, а также манипуляции данными и управляющими командами.

Один из методов несанкционированного получения информации может осуществляться с помощью специального программного обеспечения, внедряемое в компьютеры и компьютерные сети нарушая политику безопасности.

Такой метод удаленного получения информации реализуется с помощью внедрения вредоносного программного обеспечения.

Вредоносная программа (буквальный перевод англоязычного термина Malware, malicious — злонамеренный и software — программное обеспечение) — злонамеренная программа, то есть программа, созданная со злым умыслом

и/или злыми намерениями, предназначенная для обеспечения получения несанкционированного доступа к информации, хранимой на ЭВМ с целью причинения вреда (ущерба) владельцу информации и/или владельцу ЭВМ (сети ЭВМ).

Создание вредоносной программы преследует одну из двух главных целей:

- 1) получение прямой выгоды от получения доступа вредоносной программы злоумышленника (хищение конфиденциальной информации, получение доступа управлением компьютером, вымогательство и т.д.);
- 2) не приносящие прямую материальную выгоду (самоутверждение автора вредоносной программы, шутка, хулиганство).

# 1.3. Способы внедрения вредоносного программного обеспечения

Внедрения вредоносного программного обеспечения может осуществляться посредством:

- непосредственного доступа к компьютеру и его информации для последующего внедрения вредоносного ПО;
- удаленного доступа к компьютеру и внедрения вредоносного ПО;
- смешанного доступа к компьютеру, осуществляемого с помощью непосредственного и удаленного внедрения вредоносного ПО.

При этом, внедрение вредоносного ПО может быть активным и пассивным.

К активным методам внедрения относят осознанные (умышленные) методы инсталляции вредоносного ПО. Такой метод внедрения осуществляется:

- при непосредственном доступе к компьютеру пользователя достаточно инсталлировать заранее подготовленное ПО с любого съемного носителя информации, узлов локальной компьютерной сети, серверов глобальной сети Internet;
- при помощи удаленного доступа к компьютеру можно установить вредоносное ПО с помощью проникновения на компьютер благодаря неблокируемым компьютером способами (пробелам в политике безопасности).

К пассивным методам внедрения вредоносного ПО относят неумышленное проникновение на компьютер пользователя. При этом данный вид проникновения может осуществляться с помощью:

• сетевых атак со стороны зараженных компьютеров;

- непосредственного доступа к компьютеру пользователя (копирование вредоносного ПО на компьютер со съемных носителей, других зараженных узлов компьютерной сети без умышленного участия пользователей);
- социальной инженерии. Этот метод внедрения предлагает пользователю установить определенную полезную на первый взгляд программу, открыть ссылку и т.д., после чего происходит фоновое копирование на компьютер пользователя вредоносного программного обеспечения.

#### 1.4. Классификация вредоносного программного обеспечения

каждой антивирусной Как правило, у корпорации классификация согласно которой эксперты ее лаборатории определяют принадлежность нового вредоносного кода. Мы воспользуемся классификацией лаборатории Евгения Касперского. Вредоносное программное обеспечение делится на четыре большие группы, которые, в свою очередь, разделяются на классы.

#### 1.4.1. Сетевые черви

В последнее время сетевые черви, пожалуй, потеряли свою популярность среди вирусописателей. Большинство этих людей — школьники или студенты, к которым в руки тем или иным путем попадают конструкторы троянских программ. А случаи появления по-настоящему достойных экземпляров червей, которые действительно исправно выполняли бы свои вредоносные функции, сведены к минимуму. Сетевой червь — это вредоносный программный код, распространяющий свои копии по локальным или/и глобальным сетям с целью проникновения на компьютер-жертву, запуска своей копии на этом компьютере и дальнейшего распространения. Для

распространения черви используют электронную почту, ISQ, P2P- и IRC-сети, LAN, сети обмена данными между мобильными устройствами. Большинство червей распространяются в файлах (вложение в письмо, ссылка на файл и т.д.). Но существуют и черви, которые распространяются в виде сетевых пакетов. Такие разновидности проникают непосредственно в память компьютера



и сразу начинают действовать резидентно. Для проникновения на компьютержертву используются несколько путей: самостоятельный (пакетные черви), пользовательский (социальный инжиниринг), а также различные бреши в системах безопасности операционной системы и приложений. Некоторые черви обладают свойствами других типов вредоносного программного обеспечения (чаще всего это троянские программы). Теперь остановимся на классах сетевых червей.

**Почтовые черви** (Email-Worm). Данный класс сетевых червей использует для распространения электронную почту. При этом червь отправляет жертве письмо с прикрепленным телом кода либо в письме присутствует ссылка на ресурс (естественно, зараженный). Для отправки сообщений червями используются следующие способы:

- прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку;
- использование сервисов MS Outlook;
- использование функций Windows MAPI.

Для поиска адресов жертв чаще всего используется адресная книга MS Outlook, но может использоваться также адресная база WAB. Червь может просканировать файлы, хранящиеся на дисках, и выделить из них строки, относящиеся к адресам электронной почты. Черви могут отсылать свои копии по всем адресам, обнаруженным в почтовом ящике (некоторые обладают способностью отвечать на письма в ящике). Встречаются экземпляры, которые могут комбинировать способы.

**Черви, использующие интернет-пейджеры** (IM-Worm). Известные компьютерные черви данного типа используют единственный способ распространения — рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL на файл, расположенный на каком-либо вебсервере. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.

**Черви в IRC-каналах** (IRC-Worm). Черви этого класса используют два вида распространения: посылание пользователю URL-ссылки на файл-тело; отсылку пользователю файла (при этом пользователь должен подтвердить прием).

**Черви** для файлообменных сетей (P2P-Worm). Механизм работы большинства подобных червей достаточно прост: для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по его распространению P2P-сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для его скачивания с зараженного компьютера.

Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и положительно отвечают на поисковые запросы (при этом червь предлагает для скачивания свою копию).

**Прочие сетевые черви** (NET-Worm). Существуют прочие способы заражения удаленных компьютеров — например:

- копирование червя на сетевые ресурсы;
- проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
- проникновение в сетевые ресурсы публичного использования;
- паразитирование на других вредоносных программах.

Используя первый способ, червь ищет в сети машины с ресурсами, открытыми на запись, и копирует. При этом он может случайным образом находить компьютеры и пытаться открыть доступ к ресурсам. Для проникновения вторым способом червь ищет компьютеры с установленным программным обеспечением, в котором имеются критические уязвимости. Таким образом, червь отсылает специально сформированный пакет (запрос), и часть червя проникает на компьютер, после чего загружает полный файл-тело и запускает на исполнение.

#### 1.4.2. Классические вирусы

Когда профессионал говорит "вирус", он имеет в виду именно этот тип вредоносных программ. Вирусы, в отличие от червей, не пользуются сетевыми сервисами для распространения своих копий. Компьютерный вирус, как правило, попадает на компьютер-жертву по причинам, не зависящим от функционала кода. Обычно виноват пользователь, который не проверяет антивирусной программой информацию, попадающую на компьютер, в результате чего, собственно, и происходит заражение. Способов "подцепить" классический вирус довольно много:

- внешние носители информации;
- интернет ресурсы;
- файлы, распространяющиеся по сети (LAN, Internet).

Классический компьютерный вирус может иметь свойства других типов вредоносного ПО (например, троянскую процедуру удаления информации на диске). Вирусы делятся на классы по среде обитания, а эти классы, в свою очередь, делятся на подклассы по способу заражения. Итак, по среде обитания вирусы делятся на файловые, загрузочные, макро- и скриптовые. Файловые вирусы для заражения пользуются файловой системой ОС. Они различными способами внедряются в исполняемые файлы, создают файлы-двойники и т.д.

Перезаписывающие вирусы (Overwriting). Самый распространенный способ заражения. Вирус переписывает код программы (заменяет его своим), после чего, естественно, файл перестает работать. Файл, зараженный данным способом, восстановлению не подлежит. Перезаписывающий вирус быстро обнаруживает себя, так как зараженная система (или программа) перестает функционировать.

Паразитические вирусы (Parasitic). К таковым относятся все вирусы, которые изменяют содержимое файла, но при этом оставляют его работоспособным. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами — путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (cavity-вирусы). При записывании кода в начало файла вирус может воспользоваться двумя способами. Первый — это перенос начала файла в конец и дописывание собственного кода в освободившееся место. Второй дописывание кода файла к своему коду. В обоих случаях при запуске файла управление получает вирус, а потом во избежание подозрений управление передается обратно файлу-жертве. При внедрении кода вируса в конец файла используется способ дописывания. Код вируса дописывается в конец файлажертвы, при этом головная часть файла изменяется таким образом, что управление, опять же, первым получает вирус, ну, а потом файл. При внедрении в середину файла вирус может воспользоваться несколькими вариантами. Первый — перенос части файла, вместо которой предполагается расположить код вируса, в конец. Второй — так называемое "раздвижение" кода файла. Третий — замещение неисполняемых областей файла кодом вируса. Но каким бы из способов вирус ни воспользовался, ему опять придется изменять головную часть файла-жертвы. Изменение головной части кода файла происходит двумя способами. Наиболее распространен способ, при котором вирус использует точку входа, "перенося" ее на принадлежащий ему участок. Но некоторые могут просто добавить команду передачи управления — таким образом, файл стартует с оригинальной точки входа, а потом (по дописанной команде) передает управление коду вируса.

Вирусы-компаньоны (Companion). Данный способ подразумевает создание файла-двойника, при этом код файла-жертвы не изменяется. Обычно вирус изменяет расширение файла (например, с .exe на .com), потом создает свою копию с именем, идентичным имени файла-жертвы, и дает ему

расширение, тоже идентичное. Ничего не подозревающий пользователь запускает любимую программу и не подозревает, что это вирус. Вирус, в свою очередь, заражает еще несколько файлов и запускает программу, затребованную пользователем.

Незараженный файл-докунент или таблица	Вирус в файле-документе или таблице
Заголовок файла	Заголовок файла
Стужебные дамные (каталоги, FAT)	Служебные данные (каталоги, FAT)
Teker	Текст
Шрифты	Шрифты
Макросы (если есть)	Макросы (еспи еспь)
Прожие данные	Макрасы вируса
	Прочие данные

Существуют и еще способы заражения, но они настолько редко встречаются, что мы остановимся только на их перечислении: вирусы, заражающие объектные модули (OBJ); вирусы, заражающие библиотеки

компиляторов (LIB); вирусы, заражающие исходные тексты программ. Известные на текущий момент загрузочные вирусы заражают загрузочный сектор гибкого диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера — после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление. При заражении дисков загрузочные вирусы "подставляют" свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех вышеописанных способах: вирус "заставляет" систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, а коду вируса. Заражение дискет производится единственным известным способом — вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами: вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в таблице разделов диска (Disk Partition Table), расположенной в MBR винчестера. При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в какой-либо другой сектор диска (например, в первый свободный). Если длина вируса больше длины сектора, то в заражаемый сектор помещается первая часть вируса, остальные части размещаются в других секторах (например, в первых свободных). Макровирусы в основном заражают документы MS Office. При этом вирус добавляет свой код в область макросов документа. Расположение кода вируса в документах разных приложений вышеописанного пакета разное, поэтому представить его можно только лишь схематично (см. рис. 2). Скрипт-вирусы — это вирусы, написанные на скриптязыках (VBS, JS, BAT, PHP и т.д.). Заражают они файлы довольно большого диапазона расширений: от .exe до .html.

#### 1.4.3. Троянские программы

**Троянская программа** — это вредоносный код, совершающий не санкционированные пользователем действия (например, кража информации, уничтожение или модификация информации, использование ресурсов машины в злонамеренных целях и т.д.). Троянские программы являются наиболее распространенными в киберсреде, так как существует множество конструкторов, позволяющих даже неопытному пользователю создавать собственные программы данного типа.

Троянские утилиты удаленного администрирования (Backdoor). Троянские программы этого класса являются утилитами удаленного администрирования (управления) компьютеров. В общем, они очень похожи на "легальные" утилиты того же направления. Единственное, что определяет их как вредоносные программы, — это их действия без ведома пользователя. Данная программа при установке и\или загрузке не выдает никаких уведомлений. Таким образом, обладатель конкретной копии данного ПО может без ведома пользователя осуществлять операции разного рода (от выключения компьютера до манипуляций с файлами). Таким образом, троянские программы данного класса являются одними из наиболее опасных. Некоторые backdoor'ы, также могут распространяться по сети, как сетевые черви, но не самостоятельно, а после соответствующей команды владельца копии.

Похитители паролей (Trojan-PSW). Эти занимаются тем, что воруют пароли. Проникнув на компьютер и инсталлировавшись, троянец сразу приступает к поиску файлов, содержащих соответствующую информацию. Кража паролей — не основная спецификация программ этого класса — они также могут красть информацию о системе, файлы, номера счетов, коды активации другого ПО и т.д.

Интернет-кликеры (Trojan-clicker). Данное семейство троянских программ занимается организацией несанкционированных обращений к интернет-ресурсам путем отправления команд интернет-браузерам или подмены системных адресов ресурсов. Злоумышленники используют данные программы для следующих целей: увеличение посещаемости каких-либо сайтов (с целью увеличения количества показов рекламы); организация атаки на сервис; привлечение потенциальных жертв для заражения вредоносным программным обеспечением.

Загрузчики (Trojan-Downloader). Эти трояны занимаются несанкционированной загрузкой программного обеспечения (вредоносного) на компьютер ничего не подозревающего пользователя. После загрузки программа либо инсталлируется, либо записывается трояном в автозагрузку (это в зависимости от возможностей операционной системы).

Установщики (Trojan-Dropper). Эти устанавливают на компьютержертву программы — как правило, вредоносные. Анатомия троянцев этого класса следующая: основной код, файлы. Основной код собственно и является троянцем. Файлы — это программа/ы, которая/ые он должен установить. Троянец записывает ее/их в каталог (обычно временных файлов) и устанавливает. Установка происходит либо незаметно для пользователя, либо с выбросом сообщения об ошибке.

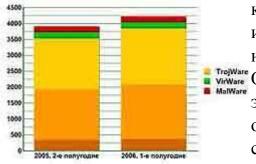
Троянские прокси-серверы (Trojan-Proxy). Семейство троянских программ, скрытно осуществляющих доступ к различным интернет-ресурсам — обычно с целью рассылки спама.

Шпионские программы (Trojan-Spy). Данные трояны осуществляют шпионаж за пользователем: записывание информации, набранной с клавиатуры, снимки экрана и т.д. В данной категории также присутствуют "многоцелевые" троянские программы — например, те из них, которые одновременно шпионят за пользователем и предоставляют ргоху-сервис удаленному злоумышленнику.

Сокрытие присутствия в операционной системе (Rootkit). Понятие гооткіт пришло к нам из UNIX. Первоначально это понятие использовалось для обозначения набора инструментов, применяемых для получения прав гоот. Так как инструменты типа rootkit на сегодняшний день "прижились" и на других ОС (в том числе на Windows), следует признать подобное определение rootkit морально устаревшим и не отвечающим реальному положению дел. Таким образом, Rootkit — программный код или техника, направленная на сокрытие присутствия в системе заданных объектов (процессов, файлов, ключей реестра и т.д.). Для поведения Rootkit в классификации "Лаборатории Касперского" действуют правила поглощения: Rootkit — самое младшее поведение среди вредоносных программ. То есть, если Rootkit-программа имеет троянскую составляющую, то она детектируется как Trojan.

Архивные бомбы (ArcBomb). Вот это интересная штука... дело в том, что такого рода архив при попытке архиватора его обработать вызывает "нестандартные" действия последнего. Компьютер может просто зависнуть или его работа существенно замедлится. Также жесткий диск может заполниться большим количеством "пустой" информации. Встречаются три типа подобных "бомб": некорректный заголовок архива, повторяющиеся данные и одинаковые файлы в архиве. Некорректный заголовок архива или испорченные данные в архиве могут привести к сбою в работе конкретного архиватора или алгоритма разархивирования при разборе содержимого архива. Значительных размеров файл, содержащий повторяющиеся данные, позволяет заархивировать такой файл в архив небольшого размера (например, 5 Гб данных упаковываются в 200 Кб RAR- или в 480 Кб ZIP-архив). Огромное количество одинаковых файлов в архиве также практически не сказывается на размере архива при использовании специальных методов (например, существуют приемы упаковки 10100 одинаковых файлов в 30 Кб RAR- или 230 Кб ZIР-архив).

Оповещение об атаке, увенчавшейся успехом (Trojan-Notifier). Троянцы данного типа предназначены для сообщения своему "хозяину" о зараженном



компьютере. При этом на адрес "хозяина" отправляется информация о компьютере — например, его ІР-адрес, номер открытого порта, адрес электронной почты и т.п. TrejWare VirWare Отсылка осуществляется различными способами: электронным письмом, специально оформленным обращением веб-странице "хозяина", ICQ-К сообщением. Данные троянские программы используются в многокомпонентных троянских наборах

для оповещения "хозяина" об успешной инсталляции троянских компонент в атакуемую систему.

#### 1.4.4. Прочие вредоносные программы

К прочим вредоносным относятся разнообразные программы, не представляющие угрозы непосредственно компьютеру, на котором исполняются, а разработанные для создания других вирусов или троянских программ, организации DoS-атак на удаленные серверы, взлома других компьютеров и т.п.

Сетевые атаки (Dos, DDoS). Эти "утилиты" используются нарушителями для организации атак на отказ в обслуживании. При выполнении атаки в адрес жертвы отправляется большое количество пакетов, в результате оборудование не справляется, и наступает так называемый "висюк". Программы данного класса бывают двух видов: первый — атака производится с компьютера злоумышленника по его приказу; второй — осуществляется распределительная атака путем заражения компьютеров (такой компьютер называется компьютером-зомби), пользователь работает в сети и при этом не подозревает, что его компьютер — участник распределительной атаки, направленной на отказ в обслуживании.

Взломщики удаленных компьютеров (Exploit, Hacktool). Эти программы используются хакерами для удаленного взлома компьютеров с целью дальнейшего управления ими. При этом эксплойты направлены непосредственно на работу с уязвимостями.

"Замусоривание" сети (Flood). Забивание интернет-каналов бесполезной информацией.

Конструкторы (Constructor). Софт, использующийся, как правило, малограмотными людьми, т.к. позволяет наиболее просто создавать троянские программы и т.д. Люди знающие обычно пишут свои.

Фатальные сетевые атаки (Nuker). Утилиты, отправляющие специально оформленные запросы на атакуемые компьютеры в сети, в результате чего атакуемая система прекращает работу. Используют уязвимости в

программном обеспечении и операционных системах, в результате чего сетевой запрос специального вида вызывает критическую ошибку в атакуемом приложении.

Введение пользователя в заблуждение (Bad-Joke, Hoax). Это, в общемто, и вредоносной программой назвать нельзя. Это программка, которая заставляет пользователя испытать страх, эквивалентный тому, который он ощущает при виде надписи типа: "Warning! System has bin delete", ну, или чтото в этом роде.

Шифровальщики вредоносного ПО (FileCryptor, PolyCryptor). Это хакерские утилиты, которые занимаются тем, что скрывают другое вредоносное ПО от антивирусных программ.

"Полиморфы" (PolyEngine). Этих вирусами можно назвать тоже с натяжкой, ведь, в принципе, в их коде не заложены действия на размножение, порчу информации и т.д. Но все же...

Вот так и выглядит современная классификация вредоносного программного обеспечения. Достаточно далеко от "стандартного" понимания того, что такое компьютерный вирус. Но теперь, видя в тревожном сообщении антивируса название обнаруженного кода, вы сможете осмысленно его прочитать и понять, что же этот конкретный код мог сделать с вашей системой или информацией. И еще: не думайте, что вредоносная программа — обязательно ужасно опасная вещь, ведь среди них встречаются и вполне безобилные.

#### 1.5. Спам

Под **спамом** (англ. spam) понимают рассылку коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать.

Укажем наиболее распространённые виды спама.

Реклама. Некоторые компании, занимающиеся легальным бизнесом, рекламируют свои товары или услуги с помощью спама. Привлекательность такой рекламы — низкая стоимость и (предположительно) большой охват потенциальных клиентов. Впрочем, такая реклама может иметь и обратный эффект, вызывая настороженность у получателей.

Реклама незаконной продукции. С помощью спама рекламируют продукцию, о которой нельзя сообщить другими способами — например, порнографию, контрафактные товары (подделки, конфискат), лекарственные средства с ограничениями по обороту, незаконно полученную закрытую информацию (базы данных), контрафактное программное обеспечение.

Сюда же относится и реклама самих услуг рассылки спама.

Антиреклама. Запрещенная законодательством о рекламе информация — например, порочащая конкурентов и их продукцию, — также может распространяться с помощью спама.

«Нигерийские письма». Иногда спам используется мошенниками, чтобы выманить деньги у получателя письма. Наиболее распространённый способ получил название «нигерийские письма», потому что большое количество таких писем приходило из Нигерии. Такое письмо содержит сообщение, якобы получатель письма может получить каким-либо образом большую сумму денег (напр. наследство однофамильца получателя), а отправитель может ему в этом помочь. Затем отправитель письма просит перевести ему относительно «немного» денег под предлогом, якобы они нужны для, например, оформления документов, или открытия счета, или для оплаты проезда или пересылочных расходов; про обещанную же крупную сумму при этом обычно говорится, якобы она пока недоступна, и выманиваемые деньги нужны для овладения ею. Выманивание этих денег и является целью мошенников.

Фишинг (англ. phishing от password — пароль и fishing — рыбалка) — ещё один способ мошенничества. Он представляет собой попытку спамеров выманить у получателя письма номера его кредитных карточек или пароли доступа к системам онлайновых платежей. Такое письмо обычно маскируется под официальное сообщение от администрации банка. В нём говорится, что получатель должен подтвердить сведения о себе, иначе его счёт будет заблокирован, и приводится адрес сайта (принадлежащего спамерам) с формой, которую надо заполнить. Среди данных, которые требуется сообщить, присутствуют и те, которые нужны мошенникам. Для того, чтобы жертва не догадалась об обмане, оформление этого сайта также имитирует оформление официального сайта банка.

Другими видами спама являются:

письма счастья;

пропаганда;

DoS и DDoS-атаки;

массовая рассылка от имени другого лица, для того чтобы вызвать к нему негативное отношение;

массовая рассылка писем, содержащих компьютерные вирусы (для их начального распространения);

рассылка писем, содержащих душещипательную историю (как правило, о больном, либо пострадавшем в результате несчастного случая ребёнке) с

информацией о том, что за каждую пересылку письма некий интернетпровайдер якобы выплатит семье пострадавшего определённую сумму денег «на лечение». Целью такой рассылки является сбор e-mail адресов: после многочисленных пересылок «всем знакомым» в тексте такого письма часто содержатся e-mail адреса всех, кому оно было переслано ранее. А в числе очередных адресатов вполне может оказаться и инициировавший её спамер.

#### 2. Методы защиты информации

#### 2.1. Правовые основы

Режим защиты компьютерной информации как комплекс правовых, организационных и технических мер, направленных на обеспечение целостности, конфиденциальности, доступности и сохранности информации должен соответствовать требованиям Закона Республики Беларусь от 10 ноября 2008 года №455-3 «Об информации, информатизации и защите информации» и обеспечиваться в отношении общедоступной информации лицом, осуществляющим распространение и (или) предоставление такой а в отношении информации, распространение и предоставление которой ограничено, — собственником или оператором информационной системы, содержащей такую информацию, информации, если такая информация не содержится в обладателем информационных системах.

В указанном законе понятие Защита информации определяется как комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации.

Целями защиты информации являются:

- обеспечение национальной безопасности, суверенитета Республики Беларусь;
- сохранение информации о частной жизни физических лиц и неразглашение персональных данных, содержащихся в информационных системах;
- обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем, сетей, технологий и ресурсов;
- недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Понятие Конфиденциальность информации определяется как требование не допускать распространения и (или) предоставления

информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь.

По доступу информация разделяется на две категории:

- общедоступная информация (о правах, свободах и законных интересах физических или юридических лиц);
- информация, распространение и (или) предоставление которой ограничено (информация о частной жизни физического лица и персональные данные; сведения, составляющие государственные секреты и т.п.).

#### 2.2. Меры по защите информации

Меры по защите информации разделяются на:

- правовые (заключение договоров);
- организационные (обеспечение особого режима допуска на территории, а также разграничение доступа к информации);
- технические (использование средств защиты информации: криптографические, контроля и регистрации фактов доступа к информации).

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля разработчиков 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.

К организационным мерам относят охрану вычислительного центра, тщательный подбор персонала, наличие плана восстановления работоспособности центра после выхода его из строя, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра и т.д.

К техническим мерам можно отнести организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку сигнализации и многое другое.

Защита от сбоев сетевого оборудования. С неисправностями сетевого кабеля и соединительных разъёмов связано почти 2/3 всех отказов в работе сети. К неисправностям кабельной системы приводят обрывы кабеля, короткое замыкание и физическое повреждение соединительных устройств.

Большие неприятности могут доставлять электромагнитные наводки различного происхождения, например, от излучения бытовых электроприборов, стартеров ламп дневного света и т. д.

Основными электрическими характеристиками кабеля, определяющими его работу, является затухание, импеданс и перекрёстные наводки. Эти характеристики позволяют определить простые и вместе с тем достаточно универсальные приборы, предназначенные для установления не только причины, но и места повреждения кабельной системы — сканеры сетевого кабеля. Современные сканеры содержат данные о номинальных параметрах распространения сигнала для сетевых кабелей различных типов, позволяют пользователю самостоятельно устанавливать такого рода параметры, а также выводить результаты тестирования на принтер.

Защита при отключении электропитания. Признанной и надёжной мерой против потерь информации, вызываемых кратковременным отключением электроэнергии, является в настоящее время установка источников бесперебойного питания. Подобные устройства, различающиеся по своим техническим и потребительским характеристикам, могут обеспечить питание отдельного компьютера в течение промежутка времени, достаточного для восстановления работы электросети или записи информации на магнитные носители.

#### 2.2.2. Программные меры защиты информации

В отдельную категорию выделим программные меры по защите информации.

Необходимо внедрять программы, с помощью которых производится мониторинг всех действий, осуществляемых на компьютерах сотрудников фирмы. Необходимо отслеживать любые движения корпоративных данных, их копирование и вывод на внешние носители. Таким образом, службы безопасности компаний имеют возможность моментально реагировать и пресекать любые несанкционированные действия, связанные с копированием информации.

Шифрование дисков (криптографические методы защиты). Зашифрованный диск — это файл-контейнер, внутри которого могут находиться любые другие файлы или программы (они могут быть установлены и запущены прямо из этого зашифрованного файла). Этот диск доступен только после ввода пароля к файлу-контейнеру — тогда на компьютере появляется еще один диск, опознаваемый системой как логический и работа с которым не отличается от работы с любым другим диском. После отключения диска логический диск исчезает, он просто становится «невидимым».

На сегодняшний день наиболее распространенными программами для создания зашифрованных дисков являются DriveCrypt, BestCrypt и PGPdisk. Каждая из них надежно защищена от удаленного взлома.

Все изменения информации в файле-контейнере происходят сначала в оперативной памяти, т.е. жесткий диск всегда остается зашифрованным. Даже в случае зависания компьютера секретные данные так и остаются зашифрованными.

Программы могут блокировать скрытый логический диск по истечении определенного промежутка времени.

Все они недоверчиво относятся к временным файлам (своп-файлам). Есть возможность зашифровать всю конфиденциальную информацию, которая могла попасть в своп-файл. Очень эффективный метод скрытия информации, хранящейся в своп-файле — это вообще отключить его, при этом, не забыв нарастить оперативную память компьютера.

Физика жесткого диска такова, что даже если поверх одних данных записать другие, то предыдущая запись полностью не сотрется. С помощью современных средств магнитной микроскопии (Magnetic Force Microscopy — MFM) их все равно можно восстановить. С помощью этих программ можно надежно удалять файлы с жесткого диска, не оставляя никаких следов их существования.

Все три программы сохраняют конфиденциальные данные в надежно зашифрованном виде на жестком диске и обеспечивают прозрачный доступ к этим данным из любой прикладной программы.

Они защищают зашифрованные файлы-контейнеры от случайного удаления.

Отлично справляются с троянскими приложениями и вирусами.

Метод парольной защиты. Проблема защиты информации решается введением контроля доступа и разграничением полномочий пользователя.

Распространённым средством ограничения доступа (или ограничения полномочий) является система паролей. Однако такой подход не всегда надежен. Опытные хакеры могут взломать эту защиту, «подсмотреть» чужой пароль или войти в систему путём перебора возможных паролей, так как очень часто для них используются имена, фамилии или даты рождения пользователей. Более надёжное решение состоит в организации контроля доступа в помещения или к конкретному ПК в ЛВС с помощью идентификационных пластиковых карточек различных видов. Более высокую степень надёжности обеспечивают пластиковые карточки со встроенной

микросхемой — так называемые микропроцессорные карточки (МП-карточки, smart-card). Их надёжность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Кроме того, при производстве карточек в каждую микросхему заносится уникальный код, который невозможно продублировать.

Установка специального считывающего устройства МП-карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

Законность запроса пользователя определяется по паролю, представляющему собой, как правило, строку знаков. Метод паролей считается достаточно слабым, так как пароль может стать объектом хищения, перехвата, перебора, угадывания. Однако простота метода стимулирует поиск путей его усиления.

Устойчивый пароль должен обладать следующими характеристиками:

- состоять, по крайней мере, из восьми символов (чем больше, тем лучше, особенно если вы хотите защитить себя от противника, располагающего значительными ресурсами);
- не должен являться словом (любого языка), которое можно встретить в словаре;
- не должен основываться на личной информации;
- должен содержать символы верхнего и нижнего регистров (а—z, A—Z);
- помимо букв желательно, чтобы в нем содержались цифры и знаки пунктуации (0...9 и любые из символов:  $!@\#\$\%^*$ \*()\_-~=\{}[]3:';"<>?>,./);
- являться легко запоминаемым для вас (чтобы его не пришлось записывать);
- использовать можно только тот пароль, который до этого никогда не записывался на бумаге или электронных носителях в незашифрованном виде.

В качестве более сложных парольных методов используется случайная выборка символов пароля и одноразовое использование паролей. В первом случае пользователю (устройству) выделяется достаточно длинный пароль, причем каждый раз для опознавания используется часть пароля, выбираемая случайно. При одноразовом использовании пароля пользователю выделяется не один, а большое количество паролей, каждый из которых используется по списку или по случайной выборке один раз.

Защита от несанкционированного доступа. В настоящее время наибольшей популярностью пользуются самые простые схемы организации защиты — системы защиты от несанкционированного доступа. Подобные системы достаточно надежны, однако не отличаются особой гибкостью. В них используются самые разные алгоритмы — от разрешения передачи сообщений

лишь с заданными адресами сетевого протокола IP до запрета прямого доступа пользователей к ресурсам Internet и интрасетям. Недостаток данной технологии кроется в узости самой постановки задачи: предотвратить доступ посторонним пользователям к внутренним сетям различного уровня. Иногда подобная защита используется для запрета доступа "особо активных" пользователей внутренних сетей, например, корпоративной сети предприятия, ко всем ресурсам Internet, за исключением обычной электронной почты. Фабула данной схемы защиты такова: неприкосновенность внутренней информации и снижение нежелательной нагрузки на внешние каналы.

Предотвращение сбоя дисковых систем. В настоящее время для восстановления данных при сбоях магнитных дисков применяются либо дублирующие друг друга зеркальные диски, либо системы дисковых массивов — Redundant Arrays of Inexpensive Disks (RAID).

Архивация данных. Организация надёжной и эффективной системы архивации данных — ещё одна важная задача по обеспечению сохранности информации. В больших ЛВС для организации резервного копирования целесообразно использовать специализированный архивационный сервер. Одной из наиболее эффективных аппаратных систем такого рода является семейство архивационных серверов StorageExpress фирмы Intel. Сервер StorageExpress подключается непосредственно к сетевому кабелю и служит для архивации данных, поступающих с любого из сетевых серверов и рабочих станций. При архивации выполняется двукратное сжатие.

Для архивной информации, представляющей особую ценность, рекомендуется предусматривать охранное помещение. Дубликаты наиболее ценных данных лучше хранить в другом здании или даже в другом городе. Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.

#### 2.2.3. Защита от вредоносных программ

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Для борьбы с компьютерными вирусами наиболее часто применяются антивирусные программы, реже — аппаратные средства защиты.

# 2.2.3.1. Виды антивирусных программ

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют

обнаруживать и уничтожать вирусы. Такие программы называются антивирусными программами.

Различают следующие виды антивирусных программ:

- 1.Программы-детекторы осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение.
- 2.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. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известными полифагами являются программы Aidstest, Scan, Norton AntiVirus и Doctor Web.
- 3.Программы-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.
- 4.Программы-фильтры, или "сторожа" представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие.
- 5.Вакцины, или иммунизаторы резидентные программы, предотвращающие заражение файлов. 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.

Современные антивирусные программы совмещают в себе средства обнаружения и защиты от вирусов.

#### 2.2.3.2. Анализ антивирусных программ



Eset Nod32 — антивирус от Словакской компании ESET. Основные преимущества — это быстрая работа и минимальная требовательность к ресурсам системы, благодаря этому быстро сканирует компьютер на наличие вирусов. Не умеет справляться с активными вирусами.

Каspersky Internet Security — российский антивирус от компании "Лаборатория Касперского". Имеет огромную функциональность для обеспечения безопасности компьютера. Распознает новейшие вирусы, обновления для него выходят каждый час. Отлично справляется с активным заражением. Из всех рассматриваемых антивирусов имеет наибольшие требования к системным ресурсам.



Norton Antivirus — антивирусная программа от компании "Symantec Corporation" с очень красивым интерфейсом. Отлично устраняет вредоносные программы, имеет отличную самозащиту. Быстро сканирует компьютер. Существенные минусы — после удаления остается много "продуктов жизнедеятельности" этой

программы, которые нужно уже удалять вручную.

Dr. Web — ещё один антивирус российской сборки. Отлично справляется с вирусами и троянами, в частности с активным заражением. Один из лучших антивирусов, защищающий свои файлы от модифицирования и проникновения в них вредоносного кода(самозащита). Достаточно функционален, но при этом чтобы



получить от него больше пользы, нужно знать как с ним работать. Плохо распознает новейшие вирусы.

Avast! Internet Security — бесплатный антивирус от Чешской компании ALWIL Software. Имеет небольшие требования к ресурсам системы, хорошо распознает все виды угроз. Существенный плюс это то, что является бесплатным. Недостаток

в том, что новые угрозы распознает позднее всех.

Avira Premium Security Suite — немецкий антивирус от компании Avira. Работает быстро, особо не заметен. Имеет хорошую защиту своих файлов. Умеет хорошо распознавать новейшие вирусы. Плохо справляется с активными и ещё не известными вредоносными программами.



Comodo Internet Security — антивирус, с хорошей самозащитой, хорошо борется с новейшими зарубежными вирусами. Неплохая проактивная защита (борьба с неизвестными вирусами). Не имеет функций для "убивания" активных вирусов.

### 2.2.3.3. Основные задачи антивирусов

Основными задачами антивирусов являются:

- сканирование файлов и программ в режиме реального времени;
- сканирование компьютера по требованию;
- сканирование интернет-трафика;
- сканирование электронной почты;
- защита от атак враждебных веб-узлов;
- восстановление поврежденных файлов (лечение).

Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню.

#### 2.2.3.4. Методы антивирусной защиты

Из всех методов антивирусной защиты можно выделить две основные группы — сигнатурные методы и эвристические методы.

Сигнатурные методы — точные методы обнаружения вирусов, файла основанные на сравнении c известными образцами вирусов. Сигнатурный анализ заключается выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами. Часто для обнаружения семейства похожих вирусов используется одна сигнатура, и поэтому считать, что количество равно количеству обнаруживаемых сигнатур вирусов, Сигнатурный метод непригоден для защиты от новых вирусов, так как до тех пор, пока вирус не попал на анализ к экспертам, создать его сигнатуру невозможно.

Эвристические методы — приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен. Эвристический анализ основывается на (весьма правдоподобном) предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных. Основанный на таком предположении эвристический метод заключается в поиске файлов, которые не полностью, но очень близко соответствуют сигнатурам известных вирусов. Положительным эффектом от

использования этого метода является возможность обнаружить новые вирусы еще до того, как для них будут выделены сигнатуры. Отрицательные стороны:

- вероятность ошибочно определить наличие в файле вируса, когда на самом деле файл чист такие события называются ложными срабатываниями;
- невозможность лечения и в силу возможных ложных срабатываний, и в силу возможного неточного определения типа вируса, попытка лечения может привести к большим потерям информации, чем сам вирус, а это недопустимо;
- низкая эффективность против действительно новаторских вирусов, вызывающих наиболее масштабные эпидемии, этот вид эвристического анализа малопригоден.

Ещё один метод основана на **поиске вирусов, выполняющих подозрительные действия**. Он основан на эвристике, исходящей из предположения, что вредоносные программы так или иначе стремятся нанести вред компьютеру. Для этого выделяют основные вредоносные действия, както:

- удаление файла;
- запись в файл;
- запись в определенные области системного реестра;
- открытие порта на прослушивание;
- перехват данных вводимых с клавиатуры;
- рассылка писем; и др.

Преимуществом этого метода является возможность обнаруживать неизвестные ранее вредоносные программы, даже если они не очень похожи на уже известные. Отрицательные черты те же, что и раньше, ложные срабатывания, невозможность лечения, невысокая эффективность.

# 2.2.3.5. Дополнительные средства

Практически любой антивирус сегодня использует все известные методы обнаружения вирусов. Но одних средств обнаружения мало для успешной работы антивируса, для того, чтобы чисто антивирусные средства были эффективными, нужны дополнительные модули, выполняющие вспомогательные функции.

**Модуль обновления.** В первую очередь, каждый антивирус должен содержать модуль обновления. После того, как эксперты создают новые сигнатуры, файлы с сигнатурами размещаются на серверах компании — производителя антивируса и становятся доступными для загрузки. Модуль обновления обращается к этим серверам, определяет наличие новых файлов, загружает их на компьютер пользователя и дает команду антивирусным модулям использовать новые файлы сигнатур.

Модули обновления разных антивирусов весьма похожи друг на друга и отличаются типами серверов, с которых они могут загружать файлы обновлений, а точнее, типами протоколов, которые они могут использовать при загрузке — HTTP, FTP, протоколы локальных Windows-сетей. Некоторые антивирусные компании создают специальные протоколы для загрузки своих обновлений антивирусной базы. Второе, в чем могут отличаться модули обновления — это настройка действий, на случай, если источник обновлений недоступен. Например, в некоторых модулях обновления можно указать не один адрес сервера с обновлениями, а адреса нескольких серверов, и модуль обновления будет обращаться к ним по очереди, пока не обнаружит работающий сервер. Или же в модуле обновления может быть настройка — повторять попытки обновления с заданным интервалом определенное количество раз или же до тех пор, пока сервер не станет доступным. Эти две настройки могут присутствовать и одновременно.

**Модуль планирования.** Существует ряд действий, которые антивирус должен выполнять регулярно: в частности, проверять весь компьютер на наличие вирусов и обновлять антивирусную базу. Модуль планирования как раз и позволяет настроить периодичность выполнения этих действий.

**Модуль управления.** По мере увеличения количества модулей в антивирусе возникает необходимость в дополнительном модуле для управления и настройки. В простейшем случае — это общий интерфейсный модуль, при помощи которого можно в удобной форме получить доступ к наиболее важным функциям:

- настройке параметров антивирусных модулей;
- настройке обновлений;
- настройке периодического запуска обновления и проверки;
- запуску модулей вручную, по требованию пользователя;
- отчётам о проверке;
- другим функциям, в зависимости от конкретного антивируса.

Основные требования к такому модулю — удобный доступ к настройкам, интуитивная понятность, подробная справочная система, описывающая каждую настройку, возможность защитить настройки от изменений, если за компьютером работает несколько человек. Подобным модулем управления обладают все антивирусы для домашнего использования. Антивирусы для защиты компьютеров в крупных сетях должны обладать несколько иными свойствами.

Уже не раз говорилось, что в большой организации за настройку и правильное функционирование антивирусов отвечают не пользователи компьютеров, а специальные сотрудники. Если компьютеров в организации

много, то каждому ответственному за безопасность сотруднику придется постоянно бегать от одного компьютера к другому, проверяя правильность настройки и просматривая историю обнаруженных заражений. Это очень неэффективный подход к обслуживанию системы безопасности.

Поэтому, чтобы упростить работу администраторов антивирусной безопасности, антивирусы, которые используются для защиты больших сетей, оборудованы специальным модулем управления. Основные свойства этого модуля управления:

поддержка удаленного управления и настройки — администратор безопасности может запускать и останавливать антивирусные модули, а также менять их настройки по сети, не вставая со своего места;

защита настроек от изменений — модуль управления не позволяет локальному пользователю изменять настройки или останавливать антивирус, чтобы пользователь не мог ослабить антивирусную защиту организации; Это далеко не все требования к управлению антивирусной защитой в крупной организации, а только основные принципы.

Карантин. Среди прочих вспомогательных средств во многих антивирусах есть специальные технологии, которые защищают от возможной потери данных в результате действий антивируса. Например, легко представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивируса. Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит с определенной вероятностью антивирус мог удалить незараженный файл. Или же антивирус обнаруживает важный документ зараженный вирусом и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченным вирусом теряется важная информация. Разумеется, от таких случаев желательно застраховаться. Проще всего это сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда если окажется, что файл был удален ошибочно или была потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

**Антивирусные комплексы.** Один из способов оптимизации работы антивируса — это создание различных его версий для компьютеров, служащих разным целям. Зачастую они отличаются лишь наличием тех или иных специфических модулей и различием в интерфейсе, в то время как непосредственно антивирусная проверка осуществляется одной и той же подпрограммой, называемой антивирусным ядром.

Антивирусный комплекс — набор антивирусов, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем. В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз.

Всякая локальная сеть, как правило, содержит компьютеры двух типов — рабочие станции, за которыми непосредственно сидят люди, и сетевые серверы, используемые для служебных целей. В соответствии с характером выполняемых функций сервера делятся на сетевые, почтовые, шлюзы.

В соответствии с этим выделяют четыре вида антивирусных комплексов — для защиты рабочих станций, для защиты файловых серверов, для защиты почтовых систем и для защиты шлюзов.

Средства защиты от нежелательной корреспонденции. Одной из наиболее многочисленных групп вредоносных программ являются почтовые черви. Также известно, что львиную долю почтовых червей составляют так называемые пассивные черви, принцип действия которых заключается в попытке обмануть пользователя и заставить его запустить зараженный файл.

Следовательно, проблема состоит в том, чтобы защитить пользователя от определенного рода нежелательных писем, похожих друг на друга. Практически аналогичным образом формулируется и проблема защиты от спама — нежелательной почты рекламного характера. И для решения этой проблемы есть специальные средства — антиспамовые фильтры, которые можно применять и для защиты от почтовых червей.

Для фильтрации нежелательной почты в антиспамовых фильтрах применяется несколько методов:

- черные и белые списки адресов;
- базы данных образцов спама;
- самообучение; антиспамовые фильтры можно "обучать", указывая вручную, какие письма являются нормальными, а какие нежелательными. Через некоторое время антиспамовый фильтр начинает с большой достоверностью самостоятельно определять нежелательные письма по их похожести на предыдущий спам и непохожести на предыдущие нормальные письма;
- анализ служебных заголовков; в письме в относительно скрытой форме хранится служебная информация о том, с какого сервера было доставлено письмо, какой адресат является реальным отправителем и др.

# 2.2.3.6. Недостатки антивирусных программ

Антивирусные программы имеют определенные недостатки:

- ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов;
- антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %;
- антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания);
- антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик;
- различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

#### 2.2.3.7. Профилактика заражения

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

копирование информации — создание копий файлов и системных областей дисков;

разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Никакие самые надежные и разумные меры не смогут обеспечить стопроцентную защиту от компьютерных вирусов и троянских программ, но, выработав для себя ряд правил, вы существенно снизите вероятность вирусной атаки и степень возможного ущерба.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика состоит

из небольшого количества правил, соблюдение которых значительно снижает вероятность заражения вирусом и потери каких-либо данных.

Ниже перечислены основные правила безопасности, выполнение которых позволит избежать риска вирусных атак.

**Правило № 1:** защитите ваш компьютер с помощью антивирусных программ и программ безопасной работы в интернете. Для этого:

Безотлагательно установите Антивирус.

- регулярно обновляйте сигнатуры угроз, входящие в состав приложения. Обновление можно проводить несколько раз в день при возникновении вирусных эпидемий;
- задайте рекомендуемые экспертами параметры защиты вашего компьютера. Защита начинает действовать сразу после включения компьютера и затрудняет вирусам проникновение на компьютер;
- задайте рекомендуемые экспертами параметры для полной проверки компьютера и запланируйте ее выполнение не реже одного раза в неделю. Если вы не установили компонент Анти-Хакер, рекомендуется сделать это, чтобы защитить компьютер при работе в интернете.

**Правило № 2:** будьте осторожны при записи новых данных на компьютер:

- проверяйте на присутствие вирусов все съемные диски (дискеты, СD-диски, флеш-карты и пр.) перед их использованием;
- осторожно обращайтесь с почтовыми сообщениями. Не запускайте никаких файлов, пришедших по почте, если вы не уверены, что они действительно должны были прийти к вам, даже если они отправлены вашими знакомыми;
- внимательно относитесь к информации, получаемой из интернета. Если с какого-либо веб-сайта вам предлагается установить новую программу, обратите внимание на наличие у нее сертификата безопасности;
- если вы копируете из интернета или локальной сети исполняемый файл, обязательно проверьте его с помощью Антивируса;
- внимательно относитесь к выбору посещаемых вами интернет-ресурсов. Некоторые из сайтов заражены опасными скрипт-вирусами или интернетчервями.

Правило № 3: внимательно относитесь к информации от Лаборатории.

В большинстве случаев Лаборатория сообщает о начале новой эпидемии задолго до того, как она достигнет своего пика. Вероятность заражения в этом случае еще невелика, и, скачав обновленные сигнатуры угроз, вы сможете защитить себя от нового вируса заблаговременно.

**Правило № 4:** с недоверием относитесь к вирусным мистификациям — программам-шуткам, письмам об угрозах заражения.

**Правило № 5:** пользуйтесь сервисом Windows Update и регулярно устанавливайте обновления операционной системы Microsoft Windows.

**Правило №6**: покупайте дистрибутивные копии программного обеспечения у официальных продавцов.

**Правило № 7**: ограничьте круг людей, допущенных к работе на вашем компьютере.

**Правило № 8:** уменьшите риск неприятных последствий возможного заражения:

- своевременно делайте резервное копирование данных. В случае потери данных система достаточно быстро может быть восстановлена при наличии резервных копий. Дистрибутивные диски, дискеты, флеш-карты и другие носители с программным обеспечением и ценной информацией должны храниться в надежном месте.
- обязательно создайте диск аварийного восстановления, с которого при необходимости можно будет загрузиться, используя «чистую» операционную систему.

Правило № 9: регулярно просматривайте список установленных на вашем компьютере программ. Для этого вы можете воспользоваться пунктом Установка/удаление программ в Панели инструментов или просто просмотреть содержимое каталога Program Files, каталога автозагрузки. Таким образом, вы можете обнаружить программное обеспечение, которое было установлено на компьютер без вашего ведома, пока вы, например, пользовались интернетом или устанавливали некоторую программу. Наверняка некоторые из них могут оказаться потенциально опасными программами.

# 2.2.3.7. Использование сервисных программ по защите, стиранию и восстановлению удаленных компьютерных данных

Программа восстановления данных PC Inspector File Recovery — простая утилита для восстановления файлов с жестких дисков и флэш-карт (Smartmedia, Compact Flash, Memory Stick и др.). Программа поддерживает файловые системы FAT 12/16/32 и NTFS и умеет восстанавливать не только случайно удаленные данные, но и информацию, утраченную после быстрого форматирования, воздействия вирусов либо повреждения файловой системы. Кроме того, она умеет выявлять невидимые в ОС логические диски. PC Inspector File Recovery поддерживает основные файловые форматы (ARJ, AVI, BMP, CDR, DOC, DXF, DBF, XLS, EXE, GIF, HLP, HTML, HTM, JPG, LZH, MID, MOV, MP3, PDF, PNG, RTF, TAR, TIF, WAV и ZIP) и потому может использоваться для восстановления документов, графических и музыкальных файлов, видеофайлов и некоторых архивов. Программу (имеется русскоязычная

локализация) можно скачать и использовать совершенно бесплатно. При каждом запуске PC Inspector File Recovery вежливо интересуется о том, какой язык интерфейса вы предпочитаете, так что о настройке русскоязычной локализации размышлять не потребуется. Но выбирать язык придется каждый раз.

#### Возможности программы:

- реконструкция поврежденных файлов;
- восстановление удаленных файлов;
- восстановление файлов после форматирования;
- программа не восстанавливает файлы, если средства хранения информации были повреждены физически.

Программа восстановления данных PC Inspector File Recovery имеет ряд аналогов: DataRecovery; EasyRecovery DataRecovery; Recover4all Professional; Back2Life; Restoration и другие.

Программа безопасного удаления данных О&O SafeErase. Многие пользователи полагают, что форматирования жесткого диска достаточно, чтобы уничтожить его содержание. Проведенное в апреле 2004 года компанией О&O исследование под названием «Данные везде» случайных жестких дисков купленных через аукционы сети Интернет показало, что в 75% случаев информация предыдущих пользователей была восстановлена программой О&O DiskRecovery.

Программа О&O SafeErase предлагает простое и эффективное решение по безопасному стиранию данных. Под безопасным стиранием подразумевается безвозвратное удаление информации с жесткого диска ПЭВМ. После применения программы SafeErase удаленная с ее помощью информация не может быть восстановлена применением специального программного обеспечения или аппаратных средств ЭВМ. Это условие необходимо учитывать, чтобы избежать ошибочного стирания данных компьютера.

В дополнение к многочисленным усовершенствованиям предыдущих версий данной программы значительно увеличен диапазон ее функциональных возможностей. Работа программы построена на окнах, в которых можно выбрать, что именно необходимо удалить, разделы на диске или же жесткие диски целиком. Этот программный инструмент так же позволяет стереть свободное место на диске, давая дополнительные гарантии по уничтожению конфиденциальной информации. Программа обладает уникальными функциональными возможностями по полному и безопасному стиранию информации (для этого необходимо запустить помощника и следовать его указаниям). После чего ваш компьютер может быть продан,

отдан или переоборудован с уверенностью, что никакие данные на нем не будут восстановлены.

SafeErase позволяет пользователю самостоятельно выбрать подходящую схему удаления информации из множества различных алгоритмов для стирания файлов. Среди предлагаемых вариантом есть алгоритмы, используемые Отделом по защите информации США (DoD), алгоритмы применяемые Немецким Федеральным Офисом по защите информации (BSI) гарантирующие высокий уровень стандарта безопасности. Используемые методы являются передовыми научно-техническими разработками в области защиты данных.

Программа О&O SafeErase имеет ряд аналогов: Tracks Eraser Pro; BCWipe; Disk Cleaner; Ccleaner и другие.

#### 2.2.4. Аппаратные методы защиты информации

В последнее время наблюдается тенденция к сочетанию программных и аппаратных методов защиты. Среди аппаратных устройств используются специальные антивирусные платы, вставленные в стандартные слоты расширения компьютера. Корпорация Intel предложила перспективную технологию защиты от вирусов в сетях, суть которой заключается в сканировании систем компьютеров еще до их загрузки.

Одним из наиболее распространенных механизмов защиты от интернетовских бандитов — "хакеров" является применение межсетевых экранов — брэндмауэров (firewalls).

Межсетевой экран — это полупроницаемая мембрана, которая располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и контролирует все информационные потоки во внутреннюю сеть и из нее.

Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

# ТЕМА 5. ПРОГРАММНЫЕ СРЕДСТВА ПРОФЕССИОНАЛЬНОГО НАЗНАЧЕНИЯ.

# Вопрос 1. Государственная система правовой информации Республики Беларусь

### 1. Понятие правовой информатизации

Под правовой информатизацией понимается процесс создания оптимальных условий для удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан на основе эффективной организации и использования информационных ресурсов с применением прогрессивных технологий.

Пути совершенствования процесса правовой информатизации общества многообразны, поэтому необходимо четкое определение целей, методов организационных форм решения поставленной задачи, т.е. формирование ее научных основ.

Правовая информатизация как процесс повышения эффективности информационного воздействия правовых норм на общественные отношения путем внедрения в правовую сферу новейших информационных технологий представляет собой одно из необходимых условий гармоничного развития общества и государства, совершенствования системы национального законодательства, особенно в условиях перехода к информационному обществу. Это предполагает включение информационных технологий в качестве составного и необходимого элемента в механизм правового регулирования, позволяющего генерировать, распространять и использовать значительные объемы правовой информации.

Главными целями правовой информатизации являются:

- информационно-правовое обеспечение внутренней деятельности органов государства;
- информационно-правовое обеспечение внешних по отношению к государственным органам субъектов, в том числе физических лиц;
- сохранение и структурирование информационного правового поля.

# 2. Государственная система правовой информации Республики Беларусь 2.1. Национальный центр правовой информации (НЦПИ).

В 1997 году на основании Указа Президента Республики Беларусь от 30 июня 1997 г. № 338 был создан Национальный центр правовой информации Республики Беларусь (НЦПИ). В соответствии с этим Указом НЦПИ является центральным государственным научно-практическим учреждением в области правовой информатизации, создания государственной системы правовой информации (ГСПИ), основанной на применении передовых информационных технологий, создания межгосударственной системы обмена правовой информацией.

Национальный центр правовой информации Республики Беларусь (НЦПИ) является центральным государственным научно-практическим учреждением, осуществляющим сбор, учет, обработку, хранение, систематизацию и актуализацию эталонной правовой информации, ее распространение (предоставление), а также официальное опубликование правовых актов.

Основными *задачами* национального центра правовой информации Республики Беларусь являются:

- создание и ведение Национального реестра правовых актов Республики Беларусь (на бумажных и электронных носителях);
- формирование и ведение единого эталонного банка данных правовой информации;
- создание и развитие государственной системы правовой информации;
- координация и непосредственная реализация работ по правовой информатизации Республики Беларусь;
- координация деятельности в области внедрения компьютерных систем и банков данных правовой информации;
- распространение правовой информации;
- участие в подготовке проектов законов и иных правовых актов в Республике Беларусь;
- проведение научных исследований в области правовой информации;
- обеспечение межгосударственного обмена правовой информацией.

В соответствии с Положением о Национальном центре правовой информации Республики Беларусь и в рамках решения основных задач НЦПИ осуществляет следующие функции:

- организационно-методическое обеспечение функционирования и развития государственной системы правовой информации Республики Беларусь, деятельности по распространению (предоставлению) правовой информации в Республике Беларусь;
- сбор правовой информации в порядке, установленном законодательством, ее учёт, обработку, хранение, систематизацию и актуализацию;
- обеспечивает ведение Национального реестра правовых актов Республики Беларусь и осуществляет издание официального периодического печатного издания «Национальный реестр правовых актов Республики Беларусь» и его электронной версии;
- формирует и ведет эталонный банк данных правовой информации и иные государственные информационно-правовые ресурсы, в том числе на договорной основе для государственных органов и иных государственных организаций банки данных, содержащие правовые акты этих органов и информацию правоприменительного характера;
- выполняет работы по формированию, ведению и обеспечению функционирования Национального правового Интернет-портала Республики Беларусь и иных государственных информационно-правовых

- ресурсов, формируемых НЦПИ и размещаемых в глобальной компьютерной сети Интернет;
- выполняет работы по ведению и сопровождению Единого правового классификатора Республики Беларусь, разрабатывает терминологические и иные словари, информационно-поисковые языки правовой тематики;
- формирует электронную библиотеку, содержащую информацию о международном праве и законодательстве иностранных государств, обеспечивает доступ к ней государственных органов и иных государственных организаций;
- осуществляет и обеспечивает распространение (предоставление) правовой информации в порядке, установленном законодательными актами;
- осуществляет анализ распространяемой в Республике Беларусь правовой информации на основании предоставляемых организациями и индивидуальными предпринимателями информационно-правовых ресурсов, печатных и электронных изданий, содержащих правовую информацию, а также доступа к информационно-правовым ресурсам, содержащим правовую информацию и размещаемым в глобальной компьютерной сети Интернет;
- по согласованию с Администрацией Президента Республики Беларусь создает региональные центры правовой информации и утверждает положения о них;
- принимает участие в организации и осуществлении межгосударственного обмена правовой информацией;
- в установленном порядке участвует в разработке проектов нормативных правовых актов по вопросам развития государственной системы правовой информации Республики Беларусь, правовой информатизации, иных актов по поручению Президента Республики Беларусь либо Администрации Президента Республики Беларусь;
- участвует в подготовке специалистов и научных кадров в области правовой информатизации в порядке, установленном законодательством;
- организует и проводит выставки, семинары, конференции и иные мероприятия, в том числе совместно с заинтересованными государственными органами и иными организациями;
- взаимодействует с государственными органами и иными организациями в целях обеспечения:
- функционирования и развития государственной системы правовой информации Республики Беларусь;
- реализации государственной политики в сфере правовой информатизации;
- эффективного использования государственных информационно-правовых ресурсов, создания условий для их развития и систематического информационного наполнения;
- развития информационных технологий в области правовой информатизации;

- реализации мероприятий, направленных на обеспечение доступа граждан и организаций к эталонной правовой информации, формирование системы правового воспитания детей и молодежи, повышение уровня правовой информированности общества в рамках государственных, региональных и иных научно-технических программ;
- осуществляет иную деятельность в соответствии с законодательством, поручениями Президента Республики Беларусь или Администрации Президента Республики Беларусь.

НЦПИ имеет свои филиалы во всех областных центрах страны и в г. Минске. У абсолютного большинства его сотрудников высшее образование, как правило, юридическое, математическое, инженерно-техническое и филологическое.

Важнейшим итогом деятельности НЦПИ является то, что за короткий срок в Беларуси создана эффективная государственная система правовой информации, основанная на использовании передовых информационных технологий. Эта система представляет собой целостный многокомпонентный механизм, позволяющий аккумулировать правовые акты, принимаемые в стране, поддерживать их в контрольном состоянии и обеспечивать эталонной правовой информацией каждого, у кого возникнет потребность в ней. В Беларуси решены вопросы консолидации потоков правовой информации в одну государственную структуру на уровне всех ветвей власти. Разработан и действует порядок обязательного и своевременного представления в НЦПИ правовых актов независимо от статуса принимающего их органа. По сути, произошла эволюция внедрения информатизации в национальное право на основе сплава современных компьютерных технологий и законодательства.

Уже через год после своего создания НЦПИ организовал оперативное обеспечение правовой информацией государственных органов, существенно расширил сферу распространения правовой информации в электронной форме, установил тесные деловые контакты с организациями соответствующего профиля в государствах-участниках СНГ и обеспечил значительное расширение межгосударственного обмена правовой информацией.

НЦПИ обеспечивает реализацию конституционного права граждан Республики Беларусь на получение полной, достоверной и своевременной правовой информации, вносит свой вклад в повышение качества нормотворческой и правоприменительной деятельности, способствует росту правовой культуры белорусского общества.

Одним из направлений деятельности НЦПИ является решение сложных и масштабных задач по совершенствованию на региональном уровне государственной системы правовой информации Республики Беларусь, механизм функционирования которой определен Указом Президента Республики Беларусь от 30 декабря 2010 г. № 712 «О совершенствовании государственной системы правовой информации Республики Беларусь».

Решение этих задач было бы невозможно без создания единой государственной сети распространения правовой информации не только в столице республики, но и в ее регионах.

Проводниками государственной политики в области правовой информатизации непосредственно на местах стали созданные в 1999 году в соответствии с Указом Президента Республики Беларусь от 30 октября 1998 г. № 524 «О мерах по совершенствованию государственной системы правовой информации» семь региональных центров правовой информации (РЦПИ), являющихся филиалами НЦПИ и входящими в его систему, которые расположены во всех областных центрах и городе Минске.

В соответствии с законодательством РЦПИ выполняют следующие функции:

- организуют на соответствующей территории распространение правовой информации в электронной и печатной форме, что гарантирует предоставление полной достоверной правовой информации всем государственным органам и организациям, а также юридическим и физическим лицам;
- формируют на договорной основе региональные банки данных правовых актов органов местного управления и самоуправления, а также банки данных иных юридических лиц;
- оказывают методическую помощь государственным органам, иным организациям и физическим лицам в работе с государственными информационно-правовыми ресурсами, формируемыми и распространяемыми НЦПИ;
- участвуют в создании сети публичных центров правовой информации, а также осуществляет координацию и методическое обеспечение их функционирования;
- участвуют в проведении научных исследований в области правовой информатизации;
- организуют и проводят выставки, обучающие семинары, конференции и иные мероприятия по правовой тематике, в том числе совместно с заинтересованными государственными органами и иными организациями.

### 2.2. Региональные центры правовой информации

Решение сложных и масштабных задач по распространению правовой информации было бы невозможно без создания единой государственной сети распространения правовой информации не только в столице республики, но и в ее регионах. Проводниками государственной политики в области правовой информатизации непосредственно на местах стали созданные во всех областных центрах и в г. Минске в 1999 году филиалы НЦПИ — региональные центры правовой информации (РЦПИ).

Функциями региональных центров правовой информации (РЦПИ) являются:

• организация на соответствующей территории распространения правовой информации;

- обеспечение ею органов местного управления и самоуправления;
- участие в:
- о создании широкой сети публичных центров правовой информации;
- о проведении практических работ по правовой информатизации региона.

# 2.2. Государственная система правовой информации Республики Беларусь

Информационно-правовая политика белорусского государства в последние годы была активно направлена на создание условий для эффективного и качественного обеспечения правовой информацией на самых разных уровнях — от государственных органов до каждого гражданина. Исходя из этого, в нашей стране было концептуально определено одно из магистральных направлений развития правовой сферы — формирование единого информационно-правового пространства путем создания государственной системы правовой информации.

НЦПИ разработана и успешно действует развивающаяся модель государственной системы правовой информации (ГСПИ), которая предназначена для удовлетворения правовых информационных потребностей государства и общества и основана на применении современных информационных технологий при накоплении, систематизации и распространении правовой информации. ГСПИ строится на информационных ресурсах НЦПИ, в составе которых в первую очередь следует выделить эталонный банк данных правовой информации (ЭБДПИ), включающий:

- банк данных «Законодательство Республики Беларусь»;
- банк данных «Международные договоры Республики Беларусь»;
- банк данных «Решения местных органов управления»;
- компьютерный банк данных проектов законов Республики Беларусь.

ГСПИ представляет собой структурированную систему, охватывающую ряд согласованных информационных, технологических и организационных процессов:

- сбор правовой информации от нормотворческих органов;
- формирование и ведение Национального реестра правовых актов Республики Беларусь в электронном виде, а также выпуск его официального издания в печатном виде<sup>4</sup>;
- формирование и ведение ЭБДПИ;
- выпуск других официальных изданий правовых актов (в частности, кодексов Республики Беларусь);
- распространение правовой информации в электронном и печатном виде;
- обеспечение функционирования и поддержка общедоступного узла Интернет (<a href="http://ncpi.gov.by">http://ncpi.gov.by</a>), содержащего сведения о законодательстве

<sup>&</sup>lt;sup>4</sup> Национальный реестр правовых актов Республики Беларусь (НРПА) в соответствии с Указом Президента Республики Беларусь от 20 июня 1998 г. № 369 «О Национальном реестре правовых актов Республики Беларусь» — это система учета правовых актов Республики Беларусь, составляющих законодательство Республики Беларусь. Ведение НРПА осуществляется на бумажных и электронных (магнитных) носителях.

Республики Беларусь и ряд других правовых информационных ресурсов, который является основой Национального правового Интернет-портала Республики Беларусь<sup>5</sup>;

- межгосударственный обмен правовой информацией.
   В настоящее время в организационную структуру ГСПИ входят:
- НЦПИ;
- узел Интернета НЦПИ;
- региональные центры правовой информации (РЦПИ);
- публичные центры правовой информации (ПЦПИ)
- юридические лица, распространяющие правовую информацию, полученную из НЦПИ<sup>6</sup>.

# 2.3. Назначение и принципы построения ГСПИ

Изначально построение ГСПИ обусловлено объективной необходимостью создания в Республике Беларусь нормативного информационно-правового ресурса, способного оперативно обеспечивать органы государственной власти и управления, юридические лица и граждан достоверной и полной информацией о действующем в республике законодательстве.

Основное *назначение* ГСПИ — оперативное обеспечение полной и достоверной правовой информацией всех государственных органов, всех юридических и физических лиц, содействие оптимизации правотворческой, правоохранительной и правоприменительной деятельности, росту правосознания и правовой культуры.

К принципам построения ГСПИ относятся:

- концентрация правовой информации, ее юридическая обработка и системный анализ в едином государственном центре НЦПИ РБ;
- проведение систематизации законодательства на основе единой для всех нормотворческих и правоприменительных органов системы классификации нормативных правовых актов;
- ведение Национального реестра правовых актов РБ (НРПА) как государственной системы учета, регистрации и опубликования правовых актов, определение перечня видов документов, включаемых в реестр, перечня государственных органов, иных организаций, которые направляют в него принятые нормативные правовые акты, и требований к оформлению (базовому формату) направляемых правовых актов;

<sup>&</sup>lt;sup>5</sup> Общегосударственная значимость функционирования Национального правового портала обозначена Указом Президента Республики Беларусь от 16 декабря 2002 г. № 609 «О Национальном правовом Интернет-портале Республики Беларусь и о внесении изменений и дополнения в Указ Президента Республики Беларусь от 30 октября 1998 г. № 524».

<sup>&</sup>lt;sup>6</sup> Указом Президента Республики Беларусь от 3 января 2002 г. № 1 были внесены изменения в порядок распространения правовой информации, и ПЦПИ определены как «пункты свободного доступа граждан к официальной правовой информации в целях формирования правовых знаний, навыков правомерного поведения, уважительного отношения к праву».

- создание единственного информационно-правового ресурса, представляющего собой эталонный банк данных правовой информации (ЭБДПИ);
- применение единого организационно-методического, программнотехнического, информационного, лингвистического научного и кадрового обеспечения на основе системно-комплексного подхода к формированию нормативно-правового ресурса;
- осуществление распространения правовых актов только на основе информации НРПА и ЭБДПИ;
- подключение к ГСПИ организаций государственной и негосударственной форм собственности в целях достижения наибольшего результата при распространении правовой информации;
- координация деятельности в области распространения правовой информации для обеспечения единых методологических подходов к распространению правовой информации и достижения единства предоставляемой нормативной правовой информации на всей территории страны и за ее пределами.

#### 2.4. Компоненты ГСПИ

ГСПИ в настоящее время состоит из следующих основных составляющих:

- 1. Национального центра правовой информации РБ центрального государственного научно-практического учреждения в области правовой информации;
- 2. автоматизированной системы формирования государственного информационного нормативно-правового ресурса, который включает:
- 3. Национального реестра правовых актов Республики Беларусь;
- 4. Эталонного банка данных правовой информации;
- 5. единого правового классификатора РБ, являющегося основой систематизации законодательства, ведения НРПА и формирования ЭБДПИ<sup>7</sup>:
- 6. комплексной системы распространения правовой информации, обеспечивающей распространение информации на электронных и бумажных носителях с использованием различных организационных и информационно-технологических форм ее распространения;
- 7. системы межгосударственного обмена правовой информацией.

В совокупности всё это образует уникальную государственную межведомственную автоматизированную систему управления правовым ресурсом, которая позволила сформировать в стране единый официальный, полный, актуализируемый, общедоступный государственный правовой информационный ресурс.

3. Национальный реестр правовых актов Республики Беларусь.

3.1. Национальный реестр правовых актов Республики Беларусь

<sup>&</sup>lt;sup>7</sup> в соответствии с Указом Президента Республики Беларусь от 4 января 1999 г. № 1 «Об утверждении Единого правового классификатора Республики Беларусь».

Национальный реестр правовых актов Республики Беларусь (Национальный реестр) создан и функционирует с 1 января 1999 г. в соответствии с Указом Президента Республики Беларусь от 20 июля 1998 г. № 369 «О Национальном реестре правовых актов Республики Беларусь».

Национальный реестр представляет собой систему учета правовых актов Республики Беларусь.

Статус Национального реестра, порядок его формирования и ведения определен Положением о Национальном реестре правовых актов Республики Беларусь, утвержденным названным Указом. Ведение Национального реестра осуществляется Национальным центром правовой информации Республики Беларусь.

Национальный реестр состоит из десяти разделов, в каждый из которых включаются правовые акты определенного вида.

Включению в национальный реестр подлежат:

- Раздел первый:
- Конституция Республики Беларусь;
- решения республиканских референдумов;
- декреты, указы, распоряжения Президента Республики Беларусь;
  - Раздел второй:
- законы Республики Беларусь;
  - Раздел третий:
- международные договоры Республики Беларусь;
  - Раздел четвертый:
- постановления Палаты представителей Национального собрания Республики Беларусь;
- постановления Совета Республики Национального собрания Республики Беларусь;
  - Раздел пятый:
  - постановления Совета Министров Республики Беларусь;
  - распоряжения Премьер-министра Республики Беларусь;
    - Раздел шестой:
- заключения и иные решения Конституционного Суда, за исключением запросов, требований и других решений процедурного характера;
- постановления Пленума Верховного Суда по вопросам применения законодательства Республики Беларусь, возникающим при рассмотрении судебных дел;
- постановления Пленума Высшего Хозяйственного Суда по вопросам применения законодательства Республики Беларусь в сфере предпринимательской и иной хозяйственной (экономической) деятельности, организационного и материально-технического обеспечения хозяйственных судов Республики Беларусь;
  - Раздел седьмой:
  - правовые акты Администрации Президента Республики Беларусь;

- нормативные правовые акты Комитета государственного контроля, Следственного комитета, Управления делами Президента Республики Беларусь, иных государственных органов, непосредственно подчиненных (подотчетных) Президенту Республики Беларусь;
  - Раздел восьмой:
- нормативные правовые акты Национального банка, Национальной академии наук Беларуси, министерств, иных республиканских органов государственного управления;
  - Раздел девятый:
- нормативные правовые акты областных, Минского городского Советов депутатов, облисполкомов, Минского горисполкома, местных Советов депутатов, исполнительных и распорядительных органов базового территориального уровня;
- решения, принятые областным, Минским городским, районным, городским (городов областного подчинения) референдумом;
- Раздел десятый:
- иные правовые акты Республики Беларусь, являющиеся нормативными.

#### 3.2. Распространение правовой информации

Правовая информация в демократическом обществе не должна носить закрытый и элитарный характер.

Распространение правовой информации представляет собой важнейшую функцию Национального центра правовой информации Республики Беларусь (НЦПИ) и основную цель создания государственной системы правовой информации.

Распространение правовой информации в стране осуществляется на основании Указа Президента Республики Беларусь от 1 декабря 1998 г. №565 «О порядке распространения правовой информации в Республике Беларусь».

Деятельность по распространению правовой информации регулируется Указом Президента Республики Беларусь от 30 декабря 2010 г. № 712 «О совершенствовании государственной системы правовой информации Республики Беларусь».

Эталонный банк данных правовой информации Республики Беларусь (ЭБДПИ) — организационно-техническая система, включающая одну или несколько баз данных аутентичных электронных копий правовых актов, а также комплекс программных, технологических, языковых и иных средств, предназначенных для их создания, ведения и использования.

Эталонный банк данных правовой информации (ЭБДПИ), формируется из правовых актов, поступающих в НЦПИ по официальной рассылке (для включения в Национальный реестр правовых актов Республики Беларусь.

С использованием единой технологии в НЦПИ ведутся следующие банки данных правовой информации:

• «Законодательство Республики Беларусь», содержащий полное собрание нормативных правовых актов в актуальном состоянии:

- декреты и указы Президента Республики Беларусь;
- законы и кодексы Республики Беларусь;
- правовые акты министерств, иных республиканских органов государственного управления, Национального банка Республики Беларусь;
- правовые акты Конституционного Суда Республики Беларусь, Верховного Суда Республики Беларусь, Высшего Хозяйственного Суда Республики Беларусь, Прокуратуры Республики Беларусь.
- «Международные договоры Республики Беларусь» (международные договоры, соглашения, конвенции, участницей которых является Республика Беларусь; правовые акты, принимаемые в рамках Союза Беларуси и России, а также СНГ и других межгосударственных образований);
- «Решения органов местного управления и самоуправления» (правовые акты областных и Минского городского Советов депутатов, областных и Минского городского исполнительных комитетов);
- Компьютерный банк данных проектов законов Республики Беларусь (проекты законов и сопроводительные документы к ним);
- «Судебная практика» (носящие нормативный характер акты Республики Конституционного Суда Беларусь, Верховного Суда Республики Беларусь, Высшего Хозяйственного Республики Суда Беларусь);
- «Распоряжения Президента и Главы Администрации Президента Республики Беларусь»;
- «Распоряжения Правительства и Премьер-министра Республики Беларусь».

#### 3.3. Способы распространения правовой информации

Как уже отмечалось во введении, основным источником правовой информации для специалистов и широкого круга граждан в настоящее время являются средства массовой информации. Это и традиционные печатные издания (газеты и журналы), и электронные СМИ (компьютерные правовые системы, радио, телевидение). Какой же из этих способов распространения правовой информации более удобен? Что перспективнее? Каковы прогнозы развития и использования различных видов СМИ для распространения правовой информации? Эти вопросы очень часто дискутируются и среди экспертов и среди обычных пользователей. Очень часто высказываются крайне радикальные взгляды: от полного неприятия компьютерных, электронных СМИ (хотя в последнее время такая точка зрения встречается все реже) до полного отрицания перспектив для изданий на бумажных носителях. Вместе с тем верный прогноз развития различных видов СМИ в этой области очень важен для своевременного и эффективного решения многих практических проблем, и в первую очередь для решения проблемы организации оперативного и качественного официального опубликования НПА.

Прежде чем детально обсудить сформулированные выше вопросы и подробно остановиться на достоинствах и недостатках различных видов СМИ, необходимо отметить следующее. Говорить об удобствах или неудобствах конкретных СМИ нельзя, не определив задачи и потребителей информации, относительно которых идет обсуждение.

#### 3.3.1. Печатные издания

Использование печатных изданий (на бумажных носителях) является традиционным способом распространения правовой информации. Вне всяких сомнений и сегодня СМИ на бумажных носителях не утратили своего значения. Несмотря на то, что компьютерные правовые системы в последние годы распространяются тиражами, сопоставимыми с тиражами традиционной периодики, роль газет и журналов нельзя недооценивать ни сейчас, ни в обозримом будущем.

Среди печатных изданий можно выделить:

сборник правовых актов «Национальный реестр правовых актов Республики Беларусь»;

сборники действующих нормативных правовых актов Президента Республики Беларусь;

сборник законодательства Республики Беларусь о трудовой и исполнительской дисциплине;

более 20 наименований официальных изданий кодексов Республики Беларусь.

Продолжая развивать выпуск правовых изданий, НЦПИ стремится в приоритетном порядке интенсивно использовать поистине безграничный потенциал современных компьютерных технологий.

#### 3.3.2. Радио и телевидение

Радио и телевидение тоже могут быть использованы для распространения правовой информации, но только с точки зрения общего правового воспитания граждан. Такие СМИ, как правило, сообщают о появлении тех или иных нормативных документов, о работе законодательной и исполнительной власти, правоохранительных и судебных органов. Мы не будем подробно обсуждать здесь использование этих СМИ, поскольку в силу своей специфики радио и телевидение не могут широко использоваться даже для ознакомления граждан с текстами правовых документов, не говоря уже о какой-либо профессиональной работе с правовой информацией.

В настоящее время в республике большое количество организаций и граждан пользуются правовой информацией В ЭЛЕКТРОННОЙ ФОРМЕ, базирующейся на эталонном банке данных правовой информации Республики Беларусь.

Производимые НЦПИ компьютерные базы данных используют в своей работе более четырехсот государственных органов, межгосударственных и зарубежных организаций.

Решение таких задач было бы невозможно без создания единой государственной сети распространения правовой информации не только в

столице республики, но и в ее регионах (региональные центры правовой информации (РЦПИ)).

#### 3.3.3. Публичные центры правовой информации

Осознавая необходимость дальнейшего развития государственной системы правовой информации, повышения правовой культуры общества и обеспечения права граждан на получение полной и достоверной правовой информации, НЦПИ выступил с инициативой создания публичных центров правовой информации (ПЦПИ) как пунктов свободного доступа граждан к официальной правовой информации.

Первым шагом в этом направлении стал Указ Президента Республики Беларусь от 1 декабря 1998 г. № 565 «О порядке распространения правовой информации в Республике Беларусь». Он возложил на государственные публичные библиотеки функцию по обеспечению свободного доступа граждан к правовой информации, опубликованной в средствах массовой информации, иных печатных изданиях или содержащейся в компьютерных базах и банках данных, в том числе через публичные центры правовой информации, созданные в этих библиотеках.

На республиканском уровне координацию и методическое обеспечение функционирования ПЦПИ осуществляют Министерство культуры Республики Беларусь, Национальная библиотека Беларуси и НЦПИ, на областном уровне — управления культуры областных и Минского городского исполнительных комитетов, областные библиотеки и региональные центры правовой информации (РЦПИ), на районном (городском) уровне — отделы культуры районных (городских) исполнительных комитетов, районные (городские) библиотеки.

В зависимости от организационной структуры библиотеки центр правовой информации может быть самостоятельным структурным подразделением, равно как входить в состав ее любого подразделения: читального зала, отдела обслуживания либо справочно-библиографического (справочно-информационного) отдела. ПЦПИ находится в подчинении директора библиотеки. В настоящее время в республике ПЦПИ действуют практически на базе всех библиотек областного и районного звеньев, около половины таких центров создано в сельской местности. Растет количество ПЦПИ, функционирующих на базе детских библиотек.

Любому пользователю независимо от возраста и социального статуса в ПЦПИ предоставлена возможность ознакомиться с текстами правовых актов, распечатать их или сохранить на отдельном носителе информации. По запросу пользователя библиотекари выполняют справки, составляют тематические списки правовых актов, предоставляют печатные и электронные издания, содержащие эталонную правовую информацию. Пользователь, не владеющий навыками работы с информационно-правовыми ресурсами, всегда может рассчитывать на помощь библиотекаря в поиске нужной информации, консультирование по вопросам работы с базами и банками данных правовой информации, интернет-ресурсами.

Создание и деятельность ПЦПИ являются наглядным примером реализации государственной политики в организации беспрепятственного доступа гражданам к официальной, достоверной и актуальной правовой информации, развития государственной системы правовой информации в нашей стране.

## 3.3.4. Национальный правовой интернет-портал Республики Беларусь

Осознавая значимость построения единого информационно-правового пространства, роль правовой культуры в развитии гражданского общества, стремясь реализовать постулаты, изложенные в основных документах и рекомендациях ООН, ЮНЕСКО и Совета Европы о доступе к информации, Окинавской хартии глобального информационного сообщества, преодолеть существующий в обществе так называемый "цифровой разрыв", Республика Беларусь предприняла реальные шаги в направлении внедрения информационных технологий в право, чем сделала доступной публичную информацию о деятельности государственных органов самому широкому кругу лиц.

Реальным свидетельством этому является создание системы распространения правовой информации в Интернете — Национальный правовой Интернет-портал Республики Беларусь (<u>www.pravo.by</u>).

Национальный правовой Интернет-портал Республики Беларусь создан в соответствии с Указом Президента Республики Беларусь от 16 декабря 2002 г. № 609 "О Национальном правовом Интернет-портале Республики Беларусь и о внесении изменений и дополнения в Указ Президента Республики Беларусь от 30 октября 1998 г. № 524".

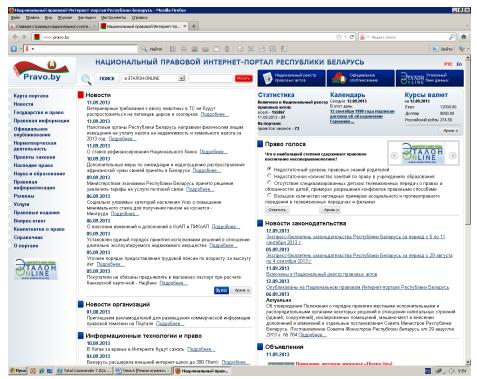
Президентом Республики Беларусь Национальный правовой Интернетпортал определен как основной государственный информационный ресурс глобальной компьютерной сети Интернет в области права и правовой информатизации.

Формирование, ведение и обеспечение функционирования Национального правового Интернет-портала осуществляются Национальным центром правовой информации.

Указом Президента Республики Беларусь от 8 января 2009 г. № 11 "О внесении изменений и дополнений в некоторые указы Президента Республики Беларусь" рассмотрение вопросов функционирования, развития и информационного наполнения Национального правового Интернет-портала возложено на Правовой консультативный совет при Президенте Республики Беларусь.

Портал представляет собой основной государственный информационный ресурс в глобальной сети Интернет в области права и правовой информатизации. Размещенная на портале информация системно представлена в 14 тематических рубриках.

Вид базовой (главной) страницы Национального правового Интернет-портала приведена на рис.1.



С этой страницы можно перейти в одну из рубрик портала, ознакомиться с последними новостями политической и правовой жизни страны и мира, просмотреть наиболее актуальный правовой акт и многое другое.

Структура этой (и всех других страниц) портала единообразна. Слева приведен перечень рубрик портала, по правой стороне содержится перечень (оглавление) ресурсов данной страницы, средняя часть отображает информацию данной рубрики (или ее подрубрики) и специфична для каждого элемента портала.

# 4. Информационно-поисковые системы по законодательству Республики Беларусь

# 4.1. Понятие информационной поисковой системы

Поиск информации — задача, которую человечество решает уже многие столетия. По мере роста объема информационных ресурсов, потенциально доступных одному человеку (например, посетителю библиотеки), были выработаны все более изощренные и совершенные поисковые средства и приемы, позволяющие найти необходимый документ.

Автоматизированная поисковая система — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Опыт и практика создания систем в различных сферах деятельности позволяет дать более широкое и универсальное определение, которое полнее отражает все аспекты их сущности.

Информационно-поисковая система (ИПС) — это система, обеспечивающая поиск и отбор необходимых данных в специальной базе с описаниями источников информации (индексе) на основе информационно-поискового языка и соответствующих правил поиска.

В настоящее время в Республике Беларусь созданы и функционируют ряд электронных информационно-поисковых, или справочно-правовых, систем. К ним относят следующие:

- 1. «КОНСУЛЬТАНТПЛЮС: БЕЛАРУСЬ», которая открывает доступ к самым разным типам правовой информации: от нормативных актов, материалов судебной практики, комментариев, законопроектов, финансовых консультаций, схем отражения операций в бухучете до бланков отчетности и узкоспециальных документов.
- 2. СИСТЕМА «ЭКСПЕРТ», представляющая собой универсальную поисковую систему со встроенной электронной библиотекой по законодательству Республики Беларусь. Более того, в системе имеются дополнительные библиотеки:
  - обзоры и комментарии квалифицированных юристов;
  - типовые формы договоров;
  - еженедельный обзор (мониторинг) изменений в законодательстве Республики Беларусь;
  - международные договоры;
  - виды экономической деятельности;
  - справочная информация (международные и междугородние телефонные коды, курсы валют, бухгалтерский словарь и др.).
- 3. ИНФОРМАЦИОННО-ПРАВОВОЕ АГЕНСТВО «РЕГИСТР», которое представляет собой юридическую справочную информационную систему правовой информации ЮСИАС. Базы данных включают белорусское и союзное законодательство, судебную и арбитражную практику, комментарии к нормативным актам, консультации, обзоры. Кроме того, агенство осуществляет подготовку и выпуск компакт-дисков правовой тематики («Кодексы Республики Беларусь», «Деловые бумаги»), издает различную правовую литературу, в том числе периодическое издание Министерства юстиции «Бюллетень нормативно-правовой информации».

Очень важно в результате проведенного поиска ничего не потерять, то есть найти все документы, относящиеся к запросу, и не найти ничего лишнего. Поэтому вводится качественная характеристика процедуры поиска — релевантность, под которой понимают соответствие результатов поиска сформулированному запросу.

# 4.2. Структура ИПС

В основу построения структуры информационно-поисковой системы легло её функциональное назначение, область применения и особенности описываемой ею предметной области.

Функционально ИПС предназначена для быстрого и удобного поиска и выборки данных из больших массивов информации по шаговым двигателям как для внутренней работы с данными, так и для подготовки их для различных САПР. Это накладывает определённые требования на построение пользовательского интерфейса и на форму предоставления информации. При

построении структуры ИПС учитывается также потребность потенциального пользователя в доступе к системе контекстно-зависимой подсказке.

Реализация вышеперечисленных требований возложена на следующий ряд структурных компонентов, так называемых блоков:

- проверки БД на целостность;
- просмотра;
- редактирования;
- защиты паролем;
- поиска;
- вывода результата;
- хранения параметров поиска;
- помощи.

В основе выбора именно такой структуры информационно-поисковой системы по шаговым двигателям лежит очень простая логика — любой блок системы должен получать данные, обрабатывать их и выдавать пользователю в определенном порядке, обеспечивая логику процесса.

*Блок проверки* БД на целостность осуществляет проверку всех составных частей базы данных.

*Блок просмотра* позволяет начать работу в системе с просмотра БД и далее выбрать другой режим работы.

*Блок редактирования* производит редактирование только числовых полей БД и позволяет изменять характеристики, вводить новые и удалять старые записи в таблицы БД. Здесь также можно произвести смену режима работы.

*Блок защиты паролем* осуществляет блокировку доступа к редактированию данных путем ввода шестизначного пароля.

*Блок поиска* предназначен для осуществления поиска по введенному техническому заданию (ТЗ) и перехода к другим режимам работы.

*Блок вывода результата* поиска выводит на экран в определенном порядке все найденные шаговые двигатели и их характеристики в соответствии с ТЗ поиска.

*Блок хранения* параметров поиска записывает и хранит информацию до следующего этапа поиска.

*Блок помощи* выполняет роль подсказки в различных режимах работы системы.

# 4.3. Информационный поиск и информационный запрос

Термин "информационный поиск" ввёл американский математик К. Муэрс. Он заметил, что побудительной причиной такого поиска является информационная потребность, выраженная в форме информационного запроса. К объектам информационного поиска К. Муэрс отнес документы, сведения об их наличии и (или) местонахождении, фактографическую информацию.

Решать проблемы фактографического поиска первыми стали представители библиотек. Они разработали средства информационного

поиска, получившие название *Справочно-поисковый аппарат* (каталоги, библиографические указатели и др.). В профессиональной отечественной печати данный термин используется с 1970-х годов. Библиотекари определяют информационный поиск как нахождение в информационном массиве документов, соответствующих информационному запросу пользователей.

С точки зрения использования компьютерной техники информационный поиск — совокупность логических и технических операций, имеющих конечной целью нахождение документов, сведений о них, фактов, данных, релевантных запросу потребителя.

Имеются и другие определения, но в любом случае, информационный поиск вызван потребностью удовлетворения информационных запросов пользователей, ожидающих с помощью поисковых систем оперативно получить необходимые им данные или сведения. Он является методом нацеленного поиска и извлечения релевантных документов и (или) фактов из различных источников информации, например, банков данных или запоминающих устройств. В качестве таковых выступают живые и неживые объекты, представляющие различные источники и носители информации.

Информационный поиск подразумевает использование определённых стратегий, методов, механизмов и средств. Поведение пользователя, осуществляющего управление процессом поиска, определяется не только информационной потребностью, но и инструментальным разнообразием системы — технологиями и средствами, предоставляемыми системой.

Стратегия поиска общий план (концепция, предпочтение, установка) поведения системы или пользователя для выражения и удовлетворения информационной потребности пользователя, обусловленный как характером цели и видом поиска, так и системными "стратегическими" решениями — архитектурой БД, методами и средствами поиска в конкретной АИПС. Выбор стратегии в общем случае является оптимизационной задачей. На практике в значительной степени он определяется искусством достижения практическими потребностями и возможностями компромисса между имеющихся средств.

*Метод поиска* — совокупность моделей и алгоритмов реализации отдельных технологических этапов — построения поискового образа запроса (ПОЗ), отбора документов (сопоставление поисковых образов запросов и документов), расширения и реформулирования запроса, локализации и оценки выдачи.

Поисковый образ запроса — записанный на информационно-поисковым языке (ИПЯ) текст, выражающий смысловое содержание информационного запроса и содержащий указания, необходимые для наиболее эффективного осуществления информационного поиска.

Вопрос 2. Информационные технологии в отдельных отраслях юридической деятельности Введение В настоящее время все большую роль в жизни общества играют информационные технологии. Большой объем информации, и необходимость быстрого ее получения требуют систематизации и возможности быстрого автоматизированного поиска и доступа к ней. Для этого создаются соответствующие базы данных и разрабатываются автоматизированные системы поиска информации. Поскольку работа правоохранительных органов всегда связана с поиском, систематизацией и отбором информации, то разработка специализированных автоматизированных систем поиска информации является очень важной составляющей успешной работы. Информатизация всех сфер деятельности, в том числе и правоохранительных органов, находят полную поддержку и со стороны государства.

## 1. Информатизация правоохранительной деятельности

В условиях современного динамичного развития экономики, производства и социальной сферы все большее значение приобретает инновационное развитие всех отраслей деятельности. В этом процессе особое значение отводится информационным технологиям.

Формирование и развитие информационного рынка страны происходит в неразрывной связи с процессами информатизации. В настоящее время в республике реализуется значительный комплекс работ, направленных на развитие и широкое применение информационных технологий в государственном и местном управлении, материальном производстве, финансовой и социальной сферах, здравоохранении, культуре.

Целью государственной политики в сфере информатизации является создание органами государственной власти необходимых правовых, экономических, организационных и других условий, обеспечивающих развитие процессов информатизации для защиты прав и законных интересов граждан и государства.

### 1.1. Совершенствование качества связи сетей национального оператора

Строительство первичных сетей национального оператора ведется с применением волоконно-оптических линий связи (ВОЛС), что обеспечивает высокое качество связи. Сегодня в республике 95 процентов протяженности междугородных телефонных каналов организовано с применением ВОЛС. Технология спектрального уплотнения каналов связи, применяемая национальным оператором электросвязи, позволяет наиболее эффективно использовать пропускную способность волоконно-оптического кабеля для развития всех сетей и услуг электросвязи.

Постоянно проводится работа по умощнению ранее построенной сети магистральных волоконно-оптических линий связи с выходом на все сопредельные государства — Польшу, Литву, Латвию, Россию, Украину. Современное оборудование систем передачи синхронной цифровой иерархии внедрено не только на внутризоновых первичных сетях, но и на городских и сельских телефонных сетях республики, что позволяет экономически эффективно развивать вторичные сети электросвязи.

Одновременно проводится модернизация телефонной сети. Уровень цифровизации коммутационного оборудования на местной телефонной сети составляет 72 процента. В настоящее время более 60 процентов абонентов электронных станций пользуются дополнительными услугами электросвязи.

Самой популярной услугой сети передачи данных является предоставление доступа в сеть Интернет, как по коммутируемым, так и по выделенным линиям связи.

Значительно возросла емкость оборудования широкополосного доступа. Узлы широкополосного доступа к сети Интернет установлены во всех районных центрах. Пользователями широкополосного доступа являются более 170 тысяч.

В Минске и областных центрах в местах общественно-политической и деловой активности организован беспроводной доступ к сети Интернет с использованием оборудования стандарта Wi-Fi. Строительство таких сетей продолжается.

С целью развития национального сегмента Интернет завершен проект по строительству центра обработки данных и его областных участков. Создана национальная площадка для физического размещения информационных ресурсов, обеспечивающая высокоскоростной доступ пользователям к этим ресурсам по сети Интернет.

Начата реализация ряда крупных взаимоувязанных проектов по модернизации инфраструктуры сетей передачи данных в целях внедрения новых услуг электросвязи:

- увеличение пропускной способности (умощнение) республиканской опорной сети передачи данных до 10 Гбит/с;
- строительство ВОЛС к жилым домам, бизнес-центрам и установка коммутаторов, позволяющих непосредственно производить подключение квартир и офисов (пользователей услуг передачи данных) на высоких скоростях к сетям передачи данных («Меtro Ethernet»);
- внедрение программно-аппаратного комплекса IP-TV, что позволит предоставлять целый спектр новых услуг: потоковое телевещание, видео по запросу и другие.

Продолжается интенсивное развитие сетей сотовой подвижной время в республике четыре электросвязи. В настоящее оказывающие услуги сотовой подвижной электросвязи в стандартах GSM 3 оператора (СООО «МТС», ИП «МЦС», ЗАО «БеСТ») и один в стандарте ІМТ-МС-450 (СП ООО «БелСел»). Общее количество абонентов превысило 7,2 миллиона. Сотовой подвижной электросвязью охвачено 89 процентов территории республики, на которой проживает более 97 процентов населения. Операторами сотовой подвижной электросвязи стандарта GSM внедрены перспективные технологии, обеспечивающие беспроводной Интернет (GPRS и EDGE), обмен мультимедийными сообщениями (MMS).

Внедрена технология 3-го поколения в стандарте CDMA EV-DO в городах Минск, Брест, Витебск, Гомель, Гродно, Могилев, Солигорск, а также Минском районе. Количество абонентов использующих эту услугу — 2,8 тысячи.

Научно-исследовательские работы разработки И ПО созданию современных информационных технологий, средств защиты информации выполняются в рамках комплексного подхода к развитию процессов информатизации в Республике Беларусь через реализацию соответствующих отраслевых государственных И программ И инициативных проектов информатизации под текущие перспективные нужды отдельных органов государственного управления и организаций.

Национальным банком и Минсвязи формируется единое расчетное и информационное пространство. Эти работы в своем развитии должны логически завершить последний этап оказания услуги в виде взимания платежей с применением информационных технологий. В конечном итоге, это является наиболее зримым и понятным результатом информатизации общества для большинства населения.

Реализация перечисленных задач обеспечит основу для следующего этапа информатизации нашей страны — системы оказания государственных информационных услуг на основе технологической инфраструктуры, обеспечивающей их широкое внедрение и территориальную доступность для различных слоев населения страны на всей территории Республики Беларусь.

### 1.2. Информатизация правоохранительной деятельности

Информация, используемая в органах внутренних дел, содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах.

В дежурных частях, у оперработников, участковых инспекторов милиции, следователей, сотрудников экспертно-криминалистических подразделений, паспортно-визовых аппаратов, других подразделений на документах первичного учета, в учетных журналах и на других носителях накапливаются массивы данных оперативно-розыскного и оперативно-справочного назначения, в которых содержатся сведения:

- о правонарушителях и преступниках;
- о владельцах автомототранспортных средств;
- о владельцах огнестрельного оружия;
- о событиях и фактах криминального характера, правонарушениях;
- о похищенных и изъятых вещах, предметах антиквариата;
- а также другая информация, подлежащая хранению.

Сами службы и подразделения органов внутренних дел характеризуются данными:

- о силах и средствах, которыми располагает орган;
- о результатах их деятельности.

Эти сведения используются при организации работы подразделений и принятии практических мер по борьбе с преступностью и правонарушениями.

Информационные центры МВД, УВД являются важнейшим звеном в системе информационного обеспечения органов внутренних дел Республики Беларусь. На них ложится основная нагрузка в обеспечении информационной поддержки органов внутренних дел в раскрытии и расследовании преступлений, розыске преступников.

Информационные центры являются головными подразделениями в системе МВД, УВД в области информатизации. Они обеспечивают статистической, оперативно-справочной, оперативно-розыскной, криминалистической, архивной и иной информацией, выполняют возложенные на них обязанности в тесном взаимодействии с подразделениями аппаратов МВД, УВД и горрайлинорганами, а также ИЦ МВД Беларуси.

Наряду с учетами в органах внутренних дел ведутся экспертнокриминалистические централизованные коллекции и картотеки, которые создаются и хранятся в экспертно-криминалистических центрах (ЭКЦ) МВД Беларуси и экспертно-криминалистических управлениях (ЭКУ) МВД, ГУВД, УВД. Коллекции и Картотеки ЭКУ и ЭКЦ ориентированы, прежде всего, на обеспечение раскрытия и расследования преступлений.

Дактилоскопический учет позволяет устанавливать личность преступников, арестованных, задержанных, а также неизвестных больных и неопознанных трупов. Дактилоскопические картотеки насчитывают 18 млн дактилокарт. В них поступает свыше 600 тыс. запросов, по которым выдается около 100 тыс. рекомендаций. Информация картотек способствовала раскрытию преступлений или установлению лица в 10 тыс. случаев.

### 3. Информатизация судебной деятельности

Дальнейшее развитие государственности на современном этапе требует укрепления судебной системы, придания ей большей оперативности и эффективности, совершенствования правового механизма обеспечения прав и свобод как физических, так и юридических лиц. Особенно это важно в условиях формирования государства для народа. Оптимальным правовым решением этой проблемы должна быть новая судебная процедура, усиливающая доступность правосудия и его качества. В основе её могут быть использованы современные информационные технологии.

Перегруженность судов в современных условиях является серьезным препятствием к повышению эффективности работы судебных органов, главными показателями которой являются оперативность и качество рассмотрения правовых споров. В последние годы количество обращений в хозяйственные суды республики значительно выросло и приблизилось к 50 тысячам. Однако, несмотря на возрастающие объем работы, сложность рассмотрения правовых споров, численность судей хозяйственных судов страны в течение восьми лет не изменялась.

Естественно, возникает вопрос, какие меры необходимо принять, чтобы избежать судебных ошибок, поверхностного, невнимательного рассмотрения дел, а также сделать наше правосудие не только качественным, но и экономичным.

Как свидетельствует судебная практика, граждане и предприниматели все в большей степени начинают верить судам и все активнее идут к судьям за защитой нарушенных прав.

В общих судах стали шире использоваться предусмотренные действующим законодательством упрощенные процедуры. В частности, по гражданским делам — приказное производство, по которому рассмотрение дел осуществляется без вызова сторон. Суд в данном случае только информирует другую сторону о заявленных к ней требованиях и выносит постановление о судебном приказе.

С учетом современных реалий наиболее оптимальной формой правосудия является электронное правосудие. В средствах массовой информации его называют «дистанционным». Как же обстоят дела в этом направлении?

Можно смело констатировать, что мы только стали приближаться к электронному правосудию. Более того, нельзя говорить об электронном правосудии, если мы не решим в полном объеме вопросы информатизации судебной деятельности, которая фактически является «матрицей» электронного правосудия.

Законом Республики Беларусь от 10 января 2000 г. № 357-3 «Об электронном документе» электронный документ на машинном носителе приравнен к документу на бумажном носителе и имеет одинаковую с ним юридическую силу (ст. 11), т. е. созданы правовые предпосылки для обращения электронного документа в соответствующей сфере. По решению Главы государства недавно к официальным источникам законодательства Республики Беларусь отнесена электронная версия издания Национального реестра правовых актов. Изучается также опыт других государств об использовании электронных документов. К примеру, в Швеции можно получить электронный документ, не выходя из дома, а судья заверяет легитимность договора своей пластиковой карточкой. Заслуживает внимания и опыт США, где государственные органы полностью ликвидировали бумажные документы, и перешли на электронный документооборот. Сейчас в республике ведется интенсивная работа по созданию общереспубликанской базы данных для обмена информацией между государственными органами.

При этом в сфере административного судопроизводства уполномоченные (несудебные) государственные органы наделены широкими субъективными правами. Они имеют право не только рассматривать дела об административных правонарушениях, но и составлять протоколы об административных правонарушениях. Это таможенные, налоговые органы, органы внутренних дел, органы Комитета государственного контроля Республики Беларусь и др.

В целях повышения оперативности и эффективности деятельности данных органов представляется целесообразным уже сегодня перейти на электронное обеспечение рассмотрения дел в сфере административных правоотношений, а также на стадии составления протоколов об

административных правонарушениях.

Как свидетельствует практика, в судах страны очень велика текучесть работников канцелярии, а также секретарей судебного заседания. Для преодоления текучести кадров в судах республики представляется целесообразным делопроизводство судов перевести на электронный документооборот. Этому способствует создание компьютерных систем протоколирования судебных заседаний, средств автоматизированного сбора и анализа первичной судебной информации. Унификация системы первичных информационных ресурсов является одним из важных условий эффективного информационного взаимодействия судов разных инстанций, следственных органов, органов прокуратуры и адвокатуры.

Современные информационные технологии позволяют, используя системный подход, решить задачи, отражающие все этапы движения и состояния дела и обеспечивающие регистрацию дел или исковых материалов и процессуальную переписку, передачу дел в архив, наработку статистических отчетов и т.д. Это позволяет руководству суда оперативно получать на экране своего компьютера (или в распечатанном виде) любые сведения о прохождении дела, группы дел, загруженности и планах судей и т.д., обеспечивая принятие ими квалифицированных и обоснованных управленческих решений.

Оболочка указанных программ должна предусматривать возможность загрузки текстового редактора «MS Word» с набором шаблонов всех процессуальных документов. При необходимости шаблоны могут редактироваться, а их библиотека — пополняться.

Шаблоны документов, будучи заложенными в систему, позволяют значительно сократить время подготовки однотипных определений, постановлений и типовых решений по делу на всех стадиях прохождения иска в суде. После окончательного их редактирования (при необходимости) и контрольного просмотра документ выводится на печать, подписывается судьей и секретарём, и подшивается.

Разумеется, решение по делу нуждается в обязательном редактировании — компьютер юридических решений не принимает и не предлагает, но предложенная технология исключает повторный набор с клавиатуры, все необходимые реквизиты вставляются в документ автоматически. Когда судья принимает решение о принятии дела к своему производству, он или по его поручению секретарь канцелярии делает необходимую пометку, и система автоматически присваивает делу учетный номер. Таким образом, за счет передачи компьютеру максимального числа технических операций удается освободить время и внимание судьи для отправления правосудия, а компьютерная технология судебного делопроизводства уже сегодня способна полностью заменить внутренний бумажный документооборот.

Использование принципиально новых информационных технологий обнаружило кроме указанных достоинств и преимуществ и ряд субъективных и объективных проблем, требующих своего последовательного решения.

К субъективным проблемам относится, прежде всего, подготовка судей и работников секретариата к использованию компьютерной техники и программного обеспечения. Эффективность работы судей существенно возрастает, что уже видно в судах, применяющих компьютерные технологии. Однако прежде чем это становится заметным, судье необходимо потратить время на обучение, что при нынешней огромной их загруженности весьма не просто сделать.

Образуется замкнутый круг — чтобы экономить время, надо его сначала потратить, а на это времени нет. В результате судьи используют лишь 10% возможностей предоставленного им программного обеспечения. Более того, многие судьи и не подозревают о широких возможностях электронных технологий, воспринимают компьютер как усовершенствованную пишущую машинку.

Ясно, что при современном уровне финансирования судебной системы, нехватки судей, их загруженности, нет возможности в сжатые сроки обучить работе с компьютером и программным обеспечением весь судейский корпус и всех работников аппарата суда. Одним из вариантов решения проблемы является, на наш взгляд, обязательное обучение указанным навыкам всех судей и канцелярских работников, впервые занимающих соответствующие должности. Полезно было бы так же в учебном плане юридических ВУЗов предусмотреть часы на обучение студентов азам работы с автоматизированной технологией судебного делопроизводства.

К объективным проблемам (помимо очевидных финансовых) следует отнести отсутствие ведомственных стандартов на структуру форм первичного учета информации, форм правовых документов и программного обеспечения. Крайне важно обеспечить единство таких стандартов не только среди пользователей судов разных уровней, но и во всей системе правоохранительных органов.

Таким образом, рассматривая состояние и последствия информатизации, можно сделать вывод, что просматривается очевидный эффект на всех уровнях системы судопроизводства: на общем и стратегическом уровне, на уровне старшего управленческого персонала судебной системы, а также на оперативном уровне.

Разумеется, мы понимаем, что сама по себе информатизация не может превратить неэффективно управляемую организацию в эффективную, но она может помочь хорошо управляемой организации работать еще более эффективно и действенно.

Преимущества информатизации прежде всего связаны с повышением эффективности самой системы судопроизводства, и поэтому обязательной предпосылкой для любой попытки информатизации является хорошая должным образом управляемая структура самой организации.

Как показывает практика, правовая информатизация охватила все отрасли права, и ее обоснованно называют промышленной революцией в праве. Эффективно функционируют мировые суды в Англии. Они рассматривают единолично и в малых сессиях (от двух до семи судей) мелкие гражданские и уголовные дела о преступлениях, за которые предусмотрено наказание в виде лишения свободы на небольшой срок или штраф.

Кодексом Республики Беларусь от 29 июня 2006 г. № 139-3 «О судоустройстве и статусе судей» не предусмотрено установление мировых судей, которые могли бы осуществлять правосудие в пределах судебных участков. Представляется также неоправданным исключение из данного Кодекса института судей по административным и исполнительным производствам и передача их функций судьям общих судов. Полагаем, что такой подход не учитывает необходимости специализировать структуры первой инстанции, которые впоследствии могут развиться в обособленные виды судебной юрисдикции. Согласно ст. 28 вышеназванного Кодекса в системе общих судов могут создаваться специализированные суды: по делам несовершеннолетних, семейные, административные и др. Однако такое решение отдается на откуп общих судов и не носит обязательного характера.

Как свидетельствует зарубежный опыт, создание административных судов улучшило бы не только защиту прав граждан, но и работу всех органов власти. Например, в Финляндии наряду с судами общей и специальной юрисдикции имеется развитая система административной юстиции. Ее возглавляет Верховный административный суд. Он состоит из президента и 21 судьи. Коллегия из 5 судей рассматривает жалобы на решения нижестоящих административных судов, именуемых судами губерний, а также на решения Государственного совета, распоряжения министров, предписания губернаторов и некоторых других исполнительных органов. Деятельность мировых, а также административных судей в Республике Беларусь существенно облегчила бы работу районных судов и могла служить мощной для подготовки судебных кадров для первичного площадкой правосудия.

Состояние правовой информатизации в Республике Беларусь позволяет сделать вывод об активизации работы в области правосудия по внедрению электронной процедуры во все судебные разбирательства с участием сторон (и уголовные, и гражданские, и хозяйственные процессы), с широким использованием интернет-технологий без обязательного присутствия сторон в зале судебного разбирательства.

Целесообразно также использовать опыт России в рассмотрении уголовных дел в особом порядке: с постановлением приговора без судебного разбирательства. Главным условием здесь для вынесения приговора в интернете должно быть признание вины подсудимым и его просьба рассмотреть дело в особом порядке.

Но как быть в случаях, когда гражданин совершил тяжкое или особо тяжкое преступление, находится вне пределов Республики Беларусь и

уклоняется от явки в суд. И здесь логично выносить приговор по интернету. Однако эти случаи должны быть четко прописаны в законодательстве.

# 4. Информационное обеспечение раскрытия и расследования преступлений

# 4.1. Информационные системы правоохранительных органов и их связь с иными информационными системами

### 4.1.1. Международные криминалистические учеты

Интерпол — международная организация уголовной полиции, созданная в 1923 и насчитывающая свыше 150 членов. Ими фактически являются, с согласия соответствующих правительств, полицейские органы входящих в него государств. Интерпол изначально создавался как организация, цель которой — борьба с международной преступностью. Ввиду разрастания и усиления транснациональных корпораций и террористических сетей координация действий подразделений уголовной полиции разных стран является насущной необходимостью.

В мировой практике борьбы с преступностью уже давно большое значение придается сбору и хранению криминалистически значимой информации, с помощью которой можно провести индивидуальное отождествление или установить групповую принадлежность проверяемого объекта в процессе раскрытия и расследования преступления (описания признаков внешности преступников, их фотографии, отпечатки пальцев и др.). В настоящее время ни одна полиция мира не обходится без налаженной службы уголовной регистрации.

Созданием международной службы уголовной регистрации Интерпола преследовались три цели:

- • аккумулировать в едином центре информацию о международных преступниках и совершенных ими преступлениях;
- добиться постоянного поступления такой информации;
- как можно шире использовать ее в процессе международного сотрудничества государств в борьбе с уголовной преступностью.

На сегодняшний день в Интерполе функционируют следующие виды криминалистических учетов:

- алфавитный (пофамильный) учет содержит сведения обо всех известных «международных преступниках» (в том числе и разыскиваемых), а также лицах, подозреваемых в преступной деятельности;
- картотека данных о внешности преступника (картотека «s»);
- картотека документов и наименований;
- картотека преступлений;
- дактилоскопическая картотека, основанная на десятипальцевой и однопальцевой регистрации;
- фототека черт внешности наиболее опасных преступников;
- картотека лиц, пропавших без вести, и неопознанных трупов;
- картотека похищенных автомашин, произведений искусства, культурных ценностей и антиквариата, дорогостоящих ювелирных изделий;

• справочная картотека ручного нарезного огнестрельного оружия.

Европол (англ. Europol) — полицейская служба Европейского союза, расположенная в Гааге. Основными задачами службы являются координация работы национальных служб в борьбе с международной организованной преступностью и улучшение информационного обмена между национальными полицейскими службами. Среди основных направлений работы Европола можно выделить борьбу с терроризмом, нелегальной торговлей оружием, наркоторговлей, детской порнографией и отмыванием денег.

На данный момент Европол координирует работу полицейских служб всех 28 стран — членов Европейского союза.

В Европоле на данный момент числятся порядка 630 сотрудников, из них около 120 **офицеров связи Европола** (англ. *Europol Liaison Officer*, *ELO*), откомандированных в Европол государствами-членами ЕС в качестве представителей их национальных правоохранительных органов.

Европол создана с целью оказания помощи правоохранительным органам ЕС в обмене криминалистически значимой информацией, анализе преступности, выработке совместных усилий в борьбе с международной преступностью. Назначение Европола заключается в совершенствовании деятельности правоохранительных органов для более эффективной борьбы с терроризмом, незаконным оборотом наркотиков и другими преступлениями, отнесенными к категории международных.

Для того чтобы выполнять свои задачи, Европол создает и обслуживает компьютеризированную информационную систему. Эта система представляет собой банк данных криминалистически значимой информации, в которую государства-члены напрямую через национальные подразделения и офицеров связи могут вводить сведения согласно своему национальному законодательству.

Постановке на криминалистический учет Европола подлежат:

- лица (подозреваемые В совершении преступлений; совершившие преступления; являющиеся соучастниками преступлений; осужденные; подозреваемые в причастности к членству в преступной организации; любые лица, которые могут быть допрошены при расследовании преступлений; потерпевшие преступлений; потенциальные OT потерпевшие, если имеются конкретные факты, свидетельствующие о том, что они могут стать таковыми; близкое окружение потерпевших, в том числе и сослуживцы; любые иные лица, потенциально предоставить какую-либо информацию о преступлении);
- преступления (совершенные и готовящиеся);
- средства, используемые при совершении преступлений.

Сотрудничество с Европолом дает нашим правоохранительным органам определенные возможности в деле борьбы с преступностью.

Во-первых, это доступ к базам данных Европола.

Во-вторых, это возможность обмена персональными данными по конкретным уголовным делам со странами ЕС. Преимуществом такого обмена станет сокращение сроков обработки информации.

В-третьих, это проведение совместных мероприятий по предотвращению деятельности транснациональных преступных группировок, занимающихся контрабандой наркотиков, изготовлением фальшивых евро и другими опасными видами преступной деятельности.

В-четвертых, это присоединение в качестве наблюдателя к проекту "КАРИН". Данный проект предусматривает создание международной сети по обмену информацией с целью изъятия и конфискации активов, полученных преступным путем, в рамках борьбы с отмыванием денег.

В-пятых, Европол с самого начала своей деятельности ориентирован на разработку аналитических проектов по противодействию различным видам преступлений.

### 4.1.2. Криминалистические учеты стран СНГ

После распада СССР организованная преступность захлестнула все Практика правовое пространство. показала, бывшего Советского правоохранительная система Союза оказалась совершенно неподготовленной к новым реалиям рыночной экономики и открытости общества. Такое положение во многом было обусловлено неправильной государственной стратегией и политикой, на которую ориентировалась правоохранительные органы СССР в течение многих десятилетий. Используя слабость и неподготовленность правоохранительных систем стран СНГ, преступные формирования действуют практически безнаказанно, развивая и контролируя такие доходные виды противоправного бизнеса, как распространение наркотиков, торговля оружием, проституция, игорный бизнес, вымогательство, мошенничество и др., агрессивно и жестоко расправляясь с противниками и конкурентами.

Выходом из сложившейся криминогенной ситуации стало стремление к объединению усилий правоохранительных органов стран СНГ в борьбе с международной преступностью. В первом десятилетии после распада Советского Союза между государствами СНГ были заключены двусторонние и многосторонние соглашения о взаимодействии в сфере борьбы с преступностью. Одним из направлений такого взаимодействия явилось участие в обмене криминалистически значимой информацией посредством формирования и функционирования межгосударственного информационного банка (МИБ) данных криминалистической информации.

Формирование МИБ осуществлялось на базе действующих централизованных оперативно-справочных и дактилоскопических учетов, а также автоматизированного банка данных криминалистических и иных учетов, в том числе и архивной информации ИЦ МВД РБ.

В настоящее время деятельность МИБ осуществляется на всей территории бывшего СССР. Его потенциал должен способствовать, в частности, информационному, организационному и оперативно-розыскному

обеспечению борьбы с различными проявлениями терроризма, контрабанды, незаконного оборота оружия и боеприпасов, незаконного оборота и использования наркотиков, противоправной деятельности организованных преступных групп и преступников-«гастролеров», действующих на территориях нескольких государств, краж грузов, перевозимых всеми видами транспорта, незаконной миграции.

На современном этапе развития системы информационного обеспечения раскрытия и расследования преступлений возможности использования криминалистически значимой информации, содержащейся в международных криминалистических учетах, приобретают все большее значение. Однако анализ отечественной научной и учебной литературы вопросам криминалистического обеспечения правоохранительной деятельности свидетельствует, что данной проблематике уделяется недостаточно внимания. По нашему мнению, в учебную литературу по криминалистике в раздел «Криминалистическая регистрация» в качестве отдельного параграфа следует включать вопросы, связанные c возможностями использования правоохранительной информации деятельности международных криминалистических учетов.

# 4.2. Информационное обеспечение раскрытия и расследования преступлений

# 4.2.1. Меры по повышению уровня информационного обеспечения раскрытия и расследования преступлений

Одной из причин недостаточного уровня раскрываемости преступлений является низкое качество информационного обеспечения процесса раскрытия и расследования преступлений. Последнее, являясь неотъемлемой частью криминалистического обеспечения, представляет собой многогранную деятельность, состоящую различных подсистем правового, ИЗ методического организационного, и технического характера. Особую приобретают развитие и дальнейшее совершенствование существующей системы криминалистических учётов, решение проблем регистрации, повышение, криминалистической эффективности информационного обеспечения правоохранительной деятельности в целом.

В настоящее время МВД осуществляет разработки и сопровождение программно-технологического обеспечения автоматизированных систем учетов, их модернизацию на базе современных специализированных высокопроизводительных вычислительных средств. Одновременно идет процесс объединения информации, сосредоточенной в различных видах криминалистических учетов в интегрированные банки данных (ИБД), что заметно повышает эффективность поисковых мероприятий, экономит время, особо ценное на первоначальном этапе расследования в условиях дефицита данных о личности виновных.

Одним из направлений развития информационного обеспечения на современном этапе является формирование новых видов криминалистических

учетов — учет запаховых следов, учет лиц на основе сведений об особенностях ДНК)

Немаловажную роль при расследовании преступлений может играть и использование возможностей глобальной компьютерной сети Интернет. Как свидетельствует зарубежная практика, Интернет оказывает большую помощь правоохранительным органам в розыске преступников.

Существующая в настоящее время система криминалистических учетов позволяет эффективно использовать содержащиеся в них сведения для раскрытия и расследования преступлений. Вместе с тем, возможности криминалистических учетов правоохранительными органами используются не в полной мере. Предложены следующие меры по повышению уровня информационного обеспечения раскрытия и расследования преступлений:

- полная автоматизация процессов обработки и выдачи необходимой информации заинтересованным лицам;
- объединение массивов криминалистически значимой информации, сосредоточенной в различных АИПС, в интегрированные банки данных (ИБД);
- формирование и внедрение в практику новых видов учетов учет запаховых следов, учет лиц на основе сведений о ДНК;
- внедрение в работу следственных подразделений программных комплексов «АРМ следователя» и их дальнейшее совершенствование;
- разработка и внедрение в практическую деятельность аналогичных АРМ для сотрудников оперативных и экспертно-криминалистических подразделений;
- создание единой формы первичных документов уголовно-статистического и криминалистического учетов;
- использование передового опыта внедрения в практику различных программно-технических комплексов, работающих с массивами криминалистически значимой информации;
- использование возможностей глобальной сети Интернет как источника криминалистически значимой информации для розыска преступников.

Информационное обеспечение раскрытия и расследования преступлений может быть рассмотрено в широком и узком смысле.

широком смысле ОНО представляет собой связь между криминалистической информацией и ее пользователем — следователем, дознавателем, оперативным работником и т.д. В узком смысле, под информационным обеспечением раскрытия и расследования преступлений следует понимать действия по выявлению и представлению (передаче) криминалистически информации непосредственному значимой ee потребителю, в том числе лицу, осуществляющему оперативно-розыскную, следственно-дознавательскую, надзорно-прокурорскую иные деятельности, сопряженные раскрытием, расследованием И предупреждением преступлений.

Информационное обеспечение представляет собой процесс с определенными, последовательно сменяющими друг друга стадиями, в котором субъекты воздействуют на объекты (информацию) для достижения конкретных результатов (целей). Процесс информационного обеспечения начинается с получения криминалистически значимой информации от ее источника или потенциального носителя. К стадиям информационного обеспечения относятся: сбор, хранение, обработка, обмен и использование информации.

Из общей задачи вытекают специальные задачи. К ним можно отнести следующие:

- обеспечение следователя, оперативного работника информацией, способствующей наиболее эффективной работе по раскрытию и расследованию, а также предупреждению преступлений;
- предупреждение и выявление административных правонарушений;
- формирование на основе собранной и обработанной информации статистических данных для криминологического анализа преступности, планирования комплексных мероприятий по борьбе с преступностью и т.д.

информационного обеспечения Весь процесс раскрытия преступлений получения первичной информации, расследования otсодержащейся в заявлениях и сообщениях о преступлениях, результатах следственных действий, оперативно-розыскных мероприятий, до передачи ее конечному пользователю — следователю, оперативному работнику, суду должен реализовываться в строгом соответствии с определенными правилами (принципами).

### 4.2.2. Криминалистическая регистрация

Криминалистическая регистрация имеет давнюю историю формирования и развития системы криминалистических учетов. В ходе исторического развития института уголовного преследования виды регистрации непрерывно совершенствовались: от клеймения и калечения до современных видов (фоноскопическая, генотипоскопическая регистрация), основанных на применении новейшей компьютерной техники.

Криминалистическая регистрация длительное время именовалась уголовной регистрацией, ибо ее основу составлял учет лиц, привлеченных к уголовной ответственности, совершенных преступлений. И ими Последовательное расширение круга учитываемых объектов (а сейчас регистрируются и лица, без вести пропавшие; трупы; предметы преступного посягательства; предметы со следами преступления; средства и способы преступлений; преступлений) следы разработанные криминалистами средства и методы получения указанной информации стали более совершенными. И совершенствуются они, главным образом, за счет внедрения современных информационных технологий.

Сейчас криминалистическая регистрация представляет собой научно обоснованную систему учёта объектов, попавших в сферу уголовного судопроизводства или оперативно-розыскной работы, для последующего

использования регистрационных данных при расследовании, розыске преступников и вещественных доказательств, а также в профилактической и аналитической работе.

В настоящее время практически ни одно уголовное дело не расследуется без информационной поддержки служб, осуществляющих ведение Информационное обеспечение криминалистических учетов. правоохранительной деятельности позволяет принимать обоснованные тактические и процессуальные решения, успешно реализовывать полученные данные.

Классификацию криминалистических учетов можно произвести по следующим основаниям:

- по территориальности;
- по функциональному признаку;
- по месту сосредоточения учетной информации.

По территориальности все учеты делятся на:

- международные учеты Интерпола, Европола, стран СНГ;
- централизованные (республиканские);
- региональные (учеты органов внутренних дел субъектов РБ);
- местные (ведутся по инициативе ГО-РОВД).

По функциональному признаку все учеты можно подразделить на:

- оперативно-справочные,
- криминалистические и розыскные;
- справочно-вспомогательные учеты.

По месту сосредоточения можно выделить:

- учеты, которые ведутся в информационных подразделениях ОВД (информационных отделениях и отделах ГО-РОВД, ГУВД, УВД и ИЦ МВД РБ);
- учеты, формирование и ведение которых возложено на экспертнокриминалистические подразделения ОВД (экспертно-криминалистические коллекции и картотеки).

В настоящее время в рамках криминалистической регистрации насчитывается более трех десятков различных видов учетов, которые в зависимости от особенностей учитываемых объектов и характеризующих их признаков можно сгруппировать по трем основным направлениям:

- оперативно-справочные, криминалистические и розыскные учеты;
- экспертно-криминалистические коллекции;
- картотеки.

Оперативно-справочные учеты позволяют быстро получать необходимые справочные и проверочные данные о задержанных лицах, еще не установленных преступниках и т.д. Эти учеты отличаются большими информационными массивами при относительно кратком (справочном) описании объекта учета.

Розыскные и криминалистические учеты, по сравнению с оперативносправочными учетами, содержат более подробные сведения об учитываемых объектах. В них содержатся не только установочные данные об объектах, но и описание их индивидуальных особенностей, а также краткое изложение обстоятельств совершенного преступления.

Экспертно-криминалистические учеты и справочно-информационные фонды необходимы для рационального и эффективного функционирования деятельности экспертных служб. Данные учеты могут быть представлены как натурными объектами, так и их копиями (в виде фотоснимков, материалов видеозаписи, слепков, оттисков), а также другими источниками криминалистически значимой информации.

К факторам, которые на практике обусловливают недостаточную эффективность использования данных криминалистических учетов, в частности, относятся:

- низкий кругозор следователей и оперативных работников в области возможностей использования АИПС;
- отсутствие полноценного контроля предоставления в АИПС учетной информации;
- низкая эффективность и некачественность методик по организации и тактике сбора информации;
- отсутствие либо недостаточность современных технических средств по обработке информации на местах;
- несовершенные каналы передачи информации и линии связи;
- текучесть кадров;
- некачественное ведение уголовных, розыскных дел и, как следствие этого, некачественный процесс выявления и сбора розыскной и доказательственной информации;
- низкий уровень учетно-регистрационной дисциплины.

# 4.2.3. Повышение эффективности информационного обеспечения правоохранительной деятельности

Можно указать такие пути решения проблем повышения эффективности информационного обеспечения правоохранительной деятельности:

- полная автоматизация процессов обработки и выдачи необходимой информации заинтересованным лицам;
- объединение массивов криминалистически значимой информации, сосредоточенной в различных АИПС, в интегрированные банки данных (ИБД);
- формирование и внедрение в практику новых видов учетов учет запаховых следов, учет лиц на основе сведений о ДНК;
- внедрение в работу следственных подразделений программных комплексов «APM следователя» и их дальнейшее совершенствование;
- разработка и внедрение в практическую деятельность аналогичных APM для сотрудников оперативных и экспертно-криминалистических подразделений;

- создание единой формы первичных документов уголовно-статистического и криминалистического учетов;
- использование передового опыта внедрения в практику различных программно-технических комплексов, работающих с массивами криминалистически значимой информации;
- использование возможностей глобальной сети Интернет как источника криминалистически значимой информации для розыска преступников.

### 4.3. Допрос с использованием средств телекоммуникации

Допрос — незаменимое следственное действие, без которого невозможно провести полное, всестороннее и объективное расследование ни одного уголовного дела. Он играет важную роль не только как преимущественно используемое средство собирания и закрепления доказательств, но и как средство проверки и оценки фактических данных в целях установления истины, в том числе как способ устранения различных нарушений уголовно-процессуального закона, допущенных в процессе расследования.

С точки зрения правового положения некоторых участников уголовного процесса было бы оправданным выделение в УПК в качестве самостоятельных видов допроса — допрос гражданского истца и гражданского ответчика как самостоятельных участников процесса, наделенных соответствующими правами, отличными зачастую от статуса таких участников процесса, как потерпевший, обвиняемый. Последние допрашиваются с учетом своего процессуального положения.

# 4.3.1. Использование системы автоматического распознавания устной речи

Некоторые новые достижения в области компьютерных технологий должны найти свое применение в практике производства допросов с использованием системы автоматического распознавания устной речи. Данная программа предназначена для быстрого введения текстов в компьютер в любом редакторе под операционную систему Windows. Самообучающаяся система способна вводить тексты со скоростью от 600 до 1000 знаков в минуту, что в несколько раз превосходит скорость любой профессиональной машинистки.

Использование такой программы было бы оправданным при проведении допросов, поскольку существенно облегчило бы работу следователя по составлению протокола. С одной стороны, распознанный в символьном выражении диалог следователя с допрашиваемым существенно бы облегчил работу по составлению протокола допроса, сведя ее к редактированию уже имеющегося текста, а с другой, предоставил бы в распоряжение следователя документ, являющийся распечаткой данных звукозаписи допроса, а значит по существу приложением к протоколу. Учитывая, что и протокол допроса и приложения к нему предъявляются допрашиваемому для ознакомления, внесения замечаний и дополнений и подписываются последним, можно

заключить, что использование системы автоматического распознавания речи допустимо при допросе.

# 4.3.2. Использование систем видео-конференц-связи 4.3.2.1. О доказательствах и правах

В гражданском процессе предусмотрена возможность разъяснения экспертами своих заключений, консультации и пояснения специалистов. Данное обстоятельство позволяет сделать вывод, что письменные разъяснения экспертами своих заключений (в ходе допроса с использованием систем видео-конференц-связи), консультации и пояснения специалистов следует относить к такой разновидности доказательств, как письменное доказательство. А устные аналоги таковых могут быть вовлечены в процесс доказывания лишь как показания свидетеля. Иные устные источники доказательств гражданским процессуальным законом не предусмотрены.

Допустимо предположить возможность фиксации разъяснений экспертами своих заключений, консультаций и пояснений специалистов с помощью аудио- и (или) видеозаписи. В этом случае появляется еще один вариант источника доказательств — аудио- и (или) видеозапись. Тем не менее, устное разъяснение экспертом своего заключения, консультация и пояснение специалиста, данные в судебном заседании, пусть и с использованием систем видео-конференц-связи, все равно остаются показаниями свидетеля и иным источником доказательств быть не могут.

Вернемся к характеристике допроса свидетеля с использованием систем видео-конференц-связи. Производство допроса в данной форме — право, а не обязанность суда. Реализуется искомое право, когда, с одной стороны, имеются фактические основания самого допроса. С другой — необходимо и возможно осуществить такой допрос путем использования систем видео-конференц-связи.

Допрос свидетеля — это судебное действие, в результате которого формируется доказательство, именуемое показаниями свидетеля. И хотя они обязательно должны фиксироваться в протоколе судебного заседания, протоколом допроса формируется все же не письменное доказательство, а показания свидетеля. Фактическим основанием допроса свидетеля являются данные о том, что лицу может быть что-нибудь известно об обстоятельствах, имеющих значение для правильного рассмотрения и разрешения дела. Указанного рода данные могут быть не только в доказательствах, но и в иного рода информации, к примеру, в сведениях, содержащихся в ходатайстве стороны.

### 4.3.2.2. Как это происходит?

В наиболее общем виде юридическое основание допроса — вызов (привод) лица на допрос либо предложение (разрешение) таковому дать показания. Причем вызов свидетеля может быть и не в суд, рассматривающий гражданское дело, а в суд, обеспечивающий участие свидетеля в судебном заседании по месту его нахождения (жительства,

пребывания), в суд, которому поручена организация допроса путем использования систем видео-конференц-связи.

До исполнения поручения о допросе свидетеля путем использования систем видео-конференц-связи осуществляется следующее:

- суд, рассматривающий гражданское дело, констатирует наличие:
  - о фактических оснований допроса данного конкретного свидетеля;
  - о необходимости (фактических оснований) производства допроса свидетеля путем использования систем видео-конференц-связи;
  - о технических возможностей организации судами видео-конференцсвязи;
- тот же самый суд выносит определение о проведении допроса свидетеля путем использования систем видео-конференц-связи;
- данным определением суд, рассматривающий гражданское дело, поручает суду по месту нахождения (жительства, пребывания) свидетеля организовать проведение допроса свидетеля путем использования систем видео-конференц-связи;
- суд по месту нахождения (жительства, пребывания) свидетеля вызывает (организует привод) к себе свидетеля.

Допустим, суд, рассматривающий гражданское дело, вынес определение об участии конкретного лица в судебном заседании путем использования систем видео-конференц-связи. Это определение направлено в суд общей юрисдикции того района, на территории которого находится (проживает, пребывает) свидетель. В данном определении помимо собственно решения о проведении допроса свидетеля путем использования систем видео-конференцсвязи указывается суд, которому дано поручение, обеспечить проведение такого допроса конкретного свидетеля. Здесь же, несомненно, указывается адрес места нахождения (жительства, пребывания) данного свидетеля.

Суд по месту нахождения (проживания, пребывания) свидетеля не производит допрос. Он лишь организовывает проведение такового. В назначенное время он вызывает свидетеля и обеспечивает возможность его допроса с использованием имеющихся у суда технических средств проведения видео-конференц-связи. Допрос свидетеля путем использования систем видео-конференц-связи осуществляет суд, в производстве которого находится гражданское дело.

Допрос свидетеля проводится по общим правилам. Перед допросом судья, председательствующий в судебном заседании суда, рассматривающего гражданское дело, обязан установить личность свидетеля, разъяснить ему права и обязанности свидетеля и предупредить об уголовной ответственности за отказ от дачи показаний и за дачу заведомо ложных показаний, взять об этом подписку. После чего выяснить отношение свидетеля к лицам, участвующим в деле, и предложить свидетелю сообщить суду все, что ему лично известно об обстоятельствах дела.

### 4.3.2.3. Принцип взаимодействия

То обстоятельство, что допрос свидетеля производится путем использования систем видео-конференц-связи, накладывает своеобразный отпечаток и на форму реализации обязанностей председательствующего суда, рассматривающего гражданское дело.

Часть из них последний реализует не лично, а опосредованно, через судью суда по месту нахождения (жительства, пребывания) допрашиваемого. Именно последний устанавливает, а затем и удостоверяет соответствие подлиннику копии паспорта (иного удостоверяющего личность документа) допрашиваемого, берет подписку у свидетелей, экспертов, переводчиков о разъяснении им судом, рассматривающим дело, прав и обязанностей и предупреждении об ответственности за их нарушение.

Остальные обязанности остаются возложенными на председательствующего рассматривающего Он путем суда, дело. использования систем видео-конференц-связи разъясняет свидетелю его права и обязанности, предупреждает об уголовной ответственности за отказ от дачи показаний и за дачу заведомо ложных показаний, выясняет отношение свидетеля к лицам, участвующим в деле, и предлагает свидетелю сообщить суду все, что ему лично известно об обстоятельствах дела.

Во время судебного разбирательства могут быть проведены повторные допросы свидетеля, в том числе и путем использования систем видеоконференц-связи. Проведение очных ставок в гражданском процессе законом не предусмотрено. Соответственно таковые не могут иметь место и при использовании рассматриваемой формы проведения судебного заседания.

#### 4.3.2.3. Фиксация показаний

Показания свидетеля заносятся в протокол судебного заседания, который ведется судом, рассматривающим гражданское дело, а не судом по месту нахождения (жительства, пребывания) свидетеля. Ведение протокола судебного действия по месту нахождения (жительства, пребывания) свидетеля не обязательно. Однако оформление такого документа не запрещено законом. Поэтому, думается, нельзя признать протокол данного судебного действия, составленный секретарем судебного заседания суда по месту нахождения (жительства, пребывания) свидетеля, а тем более показания свидетеля, в случае оформления указанного протокола недопустимыми доказательствами, основываясь лишь на том, что дача показаний свидетелем подверглась двойному протоколированию.

А вот неотражение в протоколе судебного заседания судом, рассматривающим гражданское дело, содержания показаний свидетеля, данных путем использования систем видео-конференц-связи, является прямым нарушением требований законодательства. Такое нарушение может быть причиной признания соответствующих показаний свидетеля не имеющими юридической силы.

#### 4.2 Программные средства, используемые в органах внутренних дел

1. Назначение и структура автоматизированных банков данных МВД.

- 2. Единая государственная система регистрации и учета правонарушений.
- 3. Особенности получения информации в автоматизированных банках данных МВД.

Цели лекции: ознакомиться с понятием учетов в органах внутренних дел и их основными задачами, с принципами построения учетов в органах внутренних дел, с формами ведения учетов, с назначением, структурой и принципами функционирования автоматизированных банков данных МВД, ознакомиться с понятием и основными задачами единой государственной системы регистрации и учета правонарушений (ЕГСРУП), ознакомиться с порядком регистрации правонарушений, с особенностями получения информации в автоматизированных банках данных МВД.

В соответствии с Законом Республики Беларусь «Об органах внутренних дел» основными задачами органов внутренних дел являются:

- защита жизни, здоровья, чести, достоинства, прав, свобод и законных интересов граждан, обеспечение их личной и имущественной безопасности, защита прав и законных интересов организаций;
- защита интересов общества и государства от преступных и иных противоправных посягательств, охрана общественного порядка и обеспечение общественной безопасности;
- защита собственности от преступных и иных противоправных посягательств;
- профилактика, выявление, пресечение преступлений и административных правонарушений, расследование уголовных дел, ведение административного процесса в соответствии с их компетенцией;
- розыск лиц, совершивших преступления, административные правонарушения, лиц, скрывающихся от органов, ведущих уголовный или административный процесс, лиц, уклоняющихся от отбывания наказания и иных мер уголовной ответственности, без вести пропавших и других лиц в случаях, предусмотренных законодательными актами Республики Беларусь;
- организация исполнения и отбывания наказания и иных мер уголовной ответственности, административных взысканий;
- участие в реализации государственной политики в области гражданства и миграции.

В целях решения этих задач первостепенное значение имеет сохранение гласной и негласной информации, получаемой различными службами и подразделениями органов внутренних дел в процессе служебной деятельности. Указанная информация составляет основу учетов органов внутренних дел. Учеты в органах внутренних дел в порядке, определенном нормами права, формируются и используются в пределах своей компетенции всеми службами и подразделениями милиции.

### 1. Назначение и структура автоматизированных банков данных МВД

## 1.1. Задачи и принципы построения учетов в органах внутренних дел

Учеты в органах внутренних дел — система регистрации, сосредоточения, классификации, хранения и использования сведений о соответствующих объектах учета.

В соответствии с данным определением в учете можно выделить следующие элементы:

- регистрация объекта, сведения о котором включаются в систему учета;
- фиксация сведений об объектах учета;
- сосредоточение составленных на объекты документов в определенных подразделениях и службах органов внутренних дел;
- классификация сведений об объектах учета;
- хранение сведений об объектах учета.

Рассмотрим более подробно особенности элементов учета.

**Регистрация объекта учета** — процесс, включающий в себя присвоение уполномоченными подразделениями и службами органов внутренних дел объекту учета регистрационного номера, а так же фиксацию сведений об объектах учета.

Регистрационный номер объекту учета, как правило, в большинстве учетов присваивается арабскими цифрами с возрастанием в пределах календарного года.

Существует особый порядок присвоения регистрационного номера преступлению.

**Регистрационный номер преступления** включает в себя 11 цифр и имеет следующую структуру:

- 1 и 2 цифры год регистрации преступления (последние 2 цифры года);
- 3 и 4 цифры код органа предварительного расследования (суда) (принадлежность к органам внутренних дел 01, прокуратуры 02, военной прокуратуры 03, судам 04, органам пограничной службы 05, органам государственной безопасности 06, военным судам 07, органам финансовых расследований 08, таможенным органам 09, органам государственного пожарного надзора 10, Вооруженным Силам 11);
- 5 цифра код региона (1 Минск, 2 Брестская область, 3 Витебская область, 4 Гомельская область, 5 Гродненская область, 6 Минская область, 7 Могилевская область, 8 республика, 9 транспорт);
- 6 и 7 цифры код органа предварительного расследования (суда) (устанавливается информационно-аналитическим подразделением ГУВД Минского горисполкома, УВД облисполкомов, УВД на транспорте);
- 8, 9, 10 и 11 цифры порядковый номер преступления (присваиваются в нарастающем порядке в пределах календарного года).

Фиксация сведений об объектах учета — внесение сведений об объектах учета в журналы регистрации, регистрационные карточки и (или) банки данных регистрационной информации о правонарушениях.

Фиксация сведений об объектах учета заключается:

- в выявлении общих и индивидуальных признаков объекта;
- в описании (отражении) этих признаков в документах, составляемых на объект.

В качестве индивидуализирующих признаков используются анкетные данные, сведения о внешности, следы пальцев рук, характерные особенности следов преступления, похищенных вещей и др. Каждому виду учета характерна своя система учитываемых признаков.

В зависимости от признаков объектов, положенных в основу учета, его целей и задач, применяется различные способы фиксации.

Фиксация объектов учетов в настоящее время производится следующими способами:

- описательным.
- изобразительным (фотографическим).
- дактилоскопическим.
- кодированием на магнитные носители.
- коллекционным
- смешанным (комбинированным) способами.

Сосредоточение сведений об объектах учета — направление составленных на объекты учета документов в определенные подразделения и службы органов внутренних дел.

Сосредоточение информации происходит за счет поступления в подразделения, осуществляющие учет, регистрационных карточек из подразделений органов внутренних дел.

Именно единообразный порядок сосредоточения сведений об объектах учета в органах внутренних дел во многом определяет эффективность использования этих сведений, так как сведениями можно воспользоваться только тогда, когда они сосредоточены в определенных местах, известных сотрудникам органов внутренних дел.

Сосредоточение осуществляется на четырех уровнях:

- межгосударственном (международном) (учеты Интерпола, Межгосударственного информационного банка при ГИАЦ МВД РФ и т.д.);
- государственном (в пределах Республики Беларусь);
- региональном (т.е. в пределах области, города);
- местном (территориальном) (в ГОВД, РУВД, РОВД, ОВДТ).

**Классификация сведений об объектах учета** заключается в распределении документов, в которых зафиксирована учетная информация об объекте, по группам в определенном порядке.

Очень важно не только собрать в одном месте составленные на каждый объект документы, но и систематизировать их, так как, если они будут бессистемно лежать, то найти необходимые сведения будет чрезвычайно трудно.

Для каждого вида учета выработана своя система расположения информации. Например, в учете похищенных вещей регистрационные карточки в картотеке располагаются по их наименованию, номеру, приметам.

Разработанная классификация объектов позволяет быстро определять их групповую принадлежность для помещения регистрационных материалов на объекты одного рода и вида вместе, несмотря на разновременное их получение, и обеспечивает быстрое отыскание нужных сведений по их признакам.

**Хранение сведений об объектах учета** заключается в сохранении собранной информации в течение длительного времени. При этом следует помнить, что хранение — не пассивный процесс, собранную информацию необходимо активно использовать в борьбе с преступностью.

Надо отметить, что правовыми нормами, лежащими в основе конкретного учета, регламентируется:

- назначение каждого вида учета;
- определение объектов, подлежащих постановке на учет;
- способ фиксации этих признаков в регистрационных документах;
- установление конкретной формы, в которой ведется учет;
- место сосредоточения и размещения регистрационных документов;
- порядок получения сведений об объектах, состоящих на учете: сроках, субъектах, формах запросов;
- система снятия объектов с учета;
- конкретные подразделения органов внутренних дел, на которые возлагается ведение учетов.

### Основными задачами учетов в органах внутренних дел являются:

- информационное обеспечение деятельности всех служб и подразделений правоохранительных органов;
- рациональное использование поступающей в органы внутренних дел информации;
- исключение дублирования в работе с одной и той же информацией;
- исключение необоснованных информационных потерь;
- недопущение нарушений законности в деятельности органов внутренних дел.

## В основе построения учетов в органах внутренних дел лежат следующие принципы:

- строжайшее соблюдение законности;
- полнота и достоверность учетных сведений;
- своевременность регистрации объектов;
- активное использование информационных массивов;
- научность;
- конфедициальность информации;
- экономичность.

Строгое соблюдение законности заключается в том, что организация использование данных учета В борьбе с преступностью осуществляется на основе норм нормативных правовых актов, регулирующих деятельность органов внутренних дел, и только специально на то уполномоченными сотрудниками оперативных подразделений органов внутренних дел. Строго регламентированы и формы учетов (списки, журналы, автоматизированные информационные Предусмотрены меры защиты граждан от компрометации: концентрируемые в учетах имеют узковедомственное назначение, их разглашение влечет дисциплинарную и уголовную ответственность. Четко определены сроки состояния на том или ином виде учета и основания снятия с учета. Обращение к различным массивам информации доступно только сотрудникам соответствующих подразделений и служб. Данные учета разрешается использовать исключительно в служебной деятельности.

Полнота, достоверность и своевременность регистрации объектов требует того, чтобы все объекты, представляющие оперативный интерес, брались на учет в установленные нормативными актами сроки; в учетные документы и в карточки вносились достоверные и в полном объеме сведения.

использования информационных Принцип активного массивов подразумевает осуществление комплексных многоуровневых проверок имеющейся информации об объектах учета ПО всему объему функционирующих учетов, с использованием максимально доступного числа идентифицирующих признаков, а также осуществление таких проверок незамедлительно по получении значимой информации.

Несоблюдение этих и других принципов снижает эффективность работы органов внутренних дел по быстрому и своевременному предупреждению и раскрытию преступлений.

#### Объектами учетов ОВД являются:

- лица определенных категорий и сведения о них, (например, склонные к совершению правонарушений, подготавливающие, совершающие, совершившие различные правонарушения, без вести пропавшие граждане и иные категории разыскиваемых лиц);
- неопознанные трупы людей;
- похищенные, утерянные и выявленные объекты: огнестрельное оружие, предметы антиквариата, номерные вещи и т.д.;
- различного рода следы (рук, ног, транспортных средств, орудий взлома и инструментов, применения огнестрельного оружия и т.д.);
- нераскрытые преступления, (события, факты, обстоятельства, связанные с правонарушениями);
- способы совершения преступлений;
- другие объекты и обстоятельства, имеющие значение для раскрытия, расследования и предотвращения преступлений.

В органах внутренних дел используются такие формы ведения учетов:

картотеки;

- коллекции;
- видеотеки;
- фототеки (фотоальбомы);
- дактотеки;
- журналы;
- списки;
- базы и банки данных.

В завершении, следует отметить, что информация, содержащаяся в учетах органов внутренних дел, может иметь уголовно-правовое, уголовно-процессуальное, оперативно-розыскное, административно-правовое и криминалистическое значение.

Уголовно-правовое значение имеют сведения, которые по закону влияют на характер и степень ответственности обвиняемого. Выясняемые при этом обстоятельства обычно непосредственно относятся к оценке личности преступника и влияют на решение вопроса о назначении наказания.

Уголовно-процессуальное значение учетов состоит в том, что полученные с их помощью сведения учитываются при проведении отдельных следственных действий.

Оперативно-розыскное значение имеют сведения, которые служат главным образом целям обнаружения преступников и помогают устанавливать обстоятельства, имеющие значение для раскрытия преступления;

Административно-правовое значение учетов заключается в том, что учитываемые сведения позволяют устанавливать, один раз или неоднократно совершал конкретный человек однотипные правонарушения.

*Криминалистическое значение* учетов состоит в том, что с помощью данных, сосредоточенных в них, можно установить обстоятельства, имеющее значения для изобличения преступника, доказательства его вины и успешного расследования уголовного дела.

### 1. 2. Назначение, структура и принципы функционирования автоматизированных банков данных МВД

При современном уровне информированности преступных элементов, возможности их быстрого перемещения и высокой технической оснащенности современным вооружением становится совершенно необходимым и жизненно важным, качественное изменение работы всех служб и подразделений органов внутренних дел, в том числе и за счет широкого использования современной техники, передовых информационных и телекоммуникационных технологий. Сделать это возможно единственным способом — путем использования возможностей более высокого уровня информатизации деятельности всех служб МВД, создания современных систем передачи и обмена информацией.

Эффективность борьбы с различными видами преступности, пресечение и предупреждение правонарушений во многом зависит от организации информационного обеспечения деятельности органов внутренних дел. Узловым моментом успешного решения задач, стоящих перед органами

внутренних дел, является постоянный сбор и учет всей информации, связанной с правонарушениями и преступлениями, по любым информационным срезам.

В этом немаловажную роль призваны сыграть автоматизированные банки данных и автоматизированные информационные системы органов внутренних дел.

Основы существующих автоматизированных банков данных органов внутренних дел были заложены в 70-е годы и ориентированы в направлении поддержки оперативно-служебной деятельности милиции. С учетом уровня развития программно-технических средств того периода, автоматизированные банки данных были шагом вперед по сравнению с ручными картотеками, и прежде всего решали задачи связанные с централизацией оперативнорозыскных, оперативно-справочных и статистических учетов и обеспечивали оперативное получение информации. По сути, автоматизированные банки данных были программно-технической реализацией уже существовавших учетов.

Автоматизированный банк данных (АБД) — система информационных ресурсов, программно-технических средств, организационных мероприятий по накоплению, многократной и многоцелевой обработке по единой технологии (на базе использования вычислительной техники и коммуникационных средств связи) информации об объектах учета для использования их при раскрытии и расследовании преступлений, розыске преступников и иных категорий лиц, проведении профилактических и иных мероприятий.

АБД создается на базе существующих информационных фондов ИАУ МВД, УВД облисполкомов, Мингорисполкома, УВДТ и обеспечивает накопление и обработку информации о:

- лицах;
- фактах;
- объектах, представляющих оперативный интерес.

Постановке на учет в АБД подлежат следующие лица:

- находящиеся в розыске;
- поставленные на учет по делам оперативного учета;
- психически больные, которые по заключению медицинских учреждений представляют опасность для окружающих (состоящие на специальном учете в органах здравоохранения);
- из числа профилактируемого криминогенного контингента, от которых можно ожидать совершения преступлений (наркоманы, проститутки, бродяги и т; п;) на территории области (республики);
- несовершеннолетние, содержащиеся в приемниках-распределителях;
- условно осужденные; осужденные к исправительным работам без лишения свободы; лишенные права занимать определенные должности или заниматься определенной деятельностью.

*Постановке на учет* в АБД подлежат следующие *вещи* (предметы, документы, оружие, антиквариат и т. п.):

- похищенные, обнаруженные, бесхозные, изъятые у преступников, имеющие соответствующие номера либо индивидуализирующие их признаки;
- похищенные документы общегосударственного обращения (паспорта, дипломы об образовании, водительские удостоверения и т. п.);
- огнестрельное и газовое оружие, находящееся в пользовании (собственности) организаций и граждан по разрешению органов внутренних дел.

Источник информации для АБД — сведения, содержащиеся в различных делах и материалах, полученных в результате профилактической, административной, оперативно-розыскной и следственно-криминалистической деятельности

Программно-технической основой АБД являются базы данных и системы управления базами данных.

### 1.3. Краткая характеристика и принципы функционирования баз и банков данных

Важнейшим условием обеспечения эффективного функционирования любого подразделения и органа внутренних дел в целом, является наличие развитой информационной системы, включающей в себя базы и банки данных.

В свою очередь банки данных включают в свой состав:

- вычислительную систему;
- одну или несколько баз данных.
- систему управления базами данных и набор прикладных программ.

#### Основными функциями банков данных являются:

- хранение данных и их защита (в том числе; обеспечение доступа к данным только пользователям с соответствующими полномочиями);
- модификация данных (обновление, добавление и удаление);
- поиск и отбор данных по запросам пользователей;
- вывод результатов отбора в форме, удобной пользователю.

**База данных** (**Б**Д) — совокупность взаимосвязанных данных, организованных по определенным правилам на машинных носителях.

В общем смысле термин «база данных» можно применить к любой совокупности связанной информации, объединенной вместе по определенному признаку (например, совокупность несовершеннолетних, состоящих на профилактическом учете в ИДН).

Система управления базами данных (СУБД) представляет собой совокупность программных и языковых средств, предназначенных для создания, сопровождения и использования баз данных.

По характеру использования СУБД разделяют на:

- персональные
- многопользовательские.

Многопользовательские СУБД функционируют по технологии «клиент-сервер», работают в неоднородной вычислительной среде (допускаются разные типы компьютеров и операционных систем), требуют мощных вычислительных ресурсов и имеют высокую стоимость. В органах внутренних дел в качестве многопользовательской СУБД используется Oracle. В частности с использованием данной СУБД реализован Единый государственный банк данных о правонарушениях — информационнотехническая система, находящаяся в ведении Министерства внутренних дел Республики Беларусь и включающая в себя всю совокупность сведений о правонарушениях. Разработка приложений с использованием таких СУБД требует профессиональных знаний в области программирования.

В повседневной служебной деятельности существует огромный круг задач, для которых такие вычислительные мощности не нужны. Например, сотрудник ООПП может вести автоматизированную базу данных профилактируемых лиц, сотрудник ЭКО может вести базу данных выполненных и выполняемых им экспертиз и т.п. В этом случае есть смысл воспользоваться персональными СУБД, тем более их освоение не представляет большой сложности (сравнимо с текстовыми и табличными процессорами) и выгоды от их использования очевидны.

Персональные СУБД обеспечивают возможность создания БД и недорогих приложений, работающих с этими БД.

# 2. Единая государственная система регистрации и учета правонарушений 2.1. История

Уголовный учет со времени своего возникновения очень часто менялся. В дореволюционной России основными единицами измерения считались судопроисшествие (уголовное дело, рассмотренное в суде), а также осужденный. В начале советского периода такой подход к уголовному учету в основе своей сохранился. Наряду с ним возник учет в милиции, уголовном розыске, следственно-прокурорских и других правоохранительных органах, который в каждом из этих учреждений был специфичным, так как отражал собственную служебную деятельность.

Наличие в статистическом учете разных интересов правоохранительных ведомств, его неполнота и искаженность уже в 30-е гг. подвигали к организации единого учета преступлений. Центральное статистическое управление в начале 30-х гг. предприняло опытное проведение единого карточного учета преступлений в Москве, Ленинградской области и в Крыму. Его общие принципы были изложены в специальной инструкции. Однако распространить этот опыт на всю систему уголовной юстиции тогда не удалось.

В середине 50-х гг. появились первые более или менее системные попытки регистрации не только уголовных дел и осужденных, но и преступлений. Их учет официально утвердился в 1961 г. после вступления в силу нового уголовного законодательства СССР и союзных республик. В 1965

г. была принята первая инструкция о едином учете преступлений. После этого она многократно и нередко конъюнктурно дополнялась и изменялась.

В 2006 году был принят Закон Республики Беларусь 9 января 2006 г. №94-3 «О единой государственной системе регистрации и учета правонарушений», закрепивший правовые основы единой государственной системы регистрации и учета правонарушений.

#### 2.2. Понятие, принципы и задачи

Единая государственная система регистрации и учета правонарушений (ЕГСРУП) — единый порядок регистрации правонарушений органами уголовного преследования, органами, ведущими административный процесс, и судами, а также порядок учета правонарушений и представления сведений о правонарушениях органами внутренних дел.

ЕГСРУП основывается на принципах:

- уважения и соблюдения прав, законных интересов и свобод человека и гражданина;
- законности;
- объективности, достоверности и сопоставимости информации;
- доступности и открытости информации в пределах, установленных актами законодательства Республики Беларусь;
- обязательности и единообразия регистрации и учета правонарушений. Основными задачами ЕГСРУП являются:
- сбор, обработка, обобщение, накопление, хранение и защита сведений о правонарушениях.
- предоставление сведений об объектах учета государственным органам и иным организациям Республики Беларусь, государственным органам, иным организациям иностранных государств и международным организациям, а также физическим лицам.

Регистрации и учету подлежат следующие правонарушения:

- преступления, по которым вынесены постановления об отказе в возбуждении уголовного дела в случаях, предусмотренных пунктами 3, 4, 7, 10 части 1 статьи 29 УПК Республики Беларусь;
- преступления, по которым вынесены постановления о возбуждении уголовного дела;
- преступления по уголовным делам частного обвинения, по которым постановлен и вступил в законную силу обвинительный приговор суда;
- административные правонарушения, по которым вынесены постановления о наложении административного взыскания.

### 2.3. Порядок регистрации

Порядок регистрации правонарушений органами уголовного преследования, органами, ведущими административный процесс, и судами

Регистрацию административных правонарушений осуществляют государственные органы и иные государственные организации (их территориальные структурные подразделения или органы), должностные лица

которых в соответствии с законодательством Республики Беларусь наделены полномочиями на составление протоколов об административных правонарушениях либо рассмотрение дел об административных правонарушениях, а также суды.

Регистрацию преступлений осуществляют органы предварительного расследования, прокуроры, общие суды и органы, осуществляющие исполнение наказаний.

### Порядок присвоения регистрационного номера административному правонарушению

Регистрационный номер административному правонарушению присваивается не позднее трех суток после вынесения постановления о наложении административного взыскания. Если дело об административном правонарушении подлежит передаче для рассмотрения в другой орган, ведущий административный процесс, или суд, регистрационный номер административному правонарушению присваивается регистрирующим сроки, предусмотренные статьей 10.30 Процессуальноорганом исполнительного кодекса Республики Беларусь об административных правонарушениях.

Регистрационный номер административному правонарушению присваивается арабскими цифрами с возрастанием в пределах календарного года и записывается на протоколе об административном правонарушении или постановлении о наложении административного взыскания, а также в журнале административных правонарушений. регистрации Структура регистрационного номера, присваиваемого административным правонарушениям подчиненными регистрирующими органами, определяется вышестоящим государственным органом и должна включать год регистрации административного правонарушения.

### Порядок присвоения регистрационного номера преступлению

Регистрационный номер преступлению присваивается:

- органом предварительного расследования не позднее 1 суток после вынесения постановлений:
  - о о возбуждении уголовного дела.
  - о об отказе в возбуждении уголовного дела в случаях, предусмотренных пунктами 3, 4, 7, 10 и 11 части первой статьи 29 Уголовно-процессуального кодекса Республики Беларусь.
  - о принятии к производству уголовного дела, возбужденного прокурором или поступившего от компетентного органа иностранного государства,
  - о о выделении уголовного дела;
- судом не позднее трех суток после вступления в законную силу обвинительного приговора суда по уголовному делу частного обвинения или возвращения уголовного дела из суда кассационной инстанции.

Регистрационный номер преступлению присваивается арабскими цифрами с возрастанием в пределах календарного года и фиксируется в журнале регистрации преступлений.

#### Структура регистрационного номера:

1 и 2 цифры — год регистрации преступления (последние 2 цифры года);

- 3 и 4 цифры код органа предварительного расследования (суда) (принадлежность к органам внутренних дел 01, прокуратуры 02, военной прокуратуры 03, судам 04, органам пограничной службы 05, органам государственной безопасности 06, военным судам 07, органам финансовых расследований 08, таможенным органам 09, органам государственного пожарного надзора 10, Вооруженным Силам 11);
- 5 цифра код региона (1 г. Минск, 2 Брестская область, 3 Витебская область, 4 Гомельская область, 5 Гродненская область, 6 Минская область, 7 Могилевская область, 8 республика, 9 транспорт);
- 6 и 7 цифры код органа предварительного расследования (суда) (устанавливается информационно-аналитическим подразделением главного управления внутренних дел Минского горисполкома, управлений внутренних дел облисполкомов, управления внутренних дел на транспорте);
- 8, 9, 10 и 11 цифры порядковый номер преступления (присваиваются в нарастающем порядке в пределах календарного года).

При передаче уголовного дела по подследственности в другой орган предварительного расследования регистрационный номер преступления не изменяется. Сведения о преступлении по данному делу с указанием ранее присвоенного регистрационного номера органом предварительного расследования фиксируются в журнале регистрации преступлений не позднее суток после вынесения следователем, дознавателем постановления о принятии уголовного дела к производству.

#### Фиксация сведений о правонарушениях

Сведения об административном правонарушении фиксируются в следующих регистрационных карточках:

- об административном правонарушении, совершенном физическим лицом (форма 1-AП);
- $-\,$  об административном правонарушении, совершенном юридическим лицом (форма 3-АП);
- о результатах обжалования (опротестования) вступившего в законную силу постановления по делу об административном правонарушении (форма 2-АП).

Сведения о преступлении фиксируются в следующих регистрационных карточках:

- о преступлении (форма 1);
- о физическом лице, потерпевшем в результате преступления (форма 1-П);
- о подозреваемом, обвиняемом (форма 1-Л);
- о ходе предварительного расследования (форма 2);
- об окончании предварительного расследования (форма 3);

- о лице, совершившем преступление (форма 3-Л);
- о решении прокурора по уголовному делу (форма 4);
- о ходе рассмотрения уголовного дела в суде (форма 5);
- о лице, заключенном под стражу, осужденном (форма 6);
- о месте нахождения осужденного (форма 7).

Регистрационные карточки печатаются с использованием электронновычислительной техники. В тексте могут использоваться только общепринятые аббревиатуры, сокращения и термины.

Допускается заполнение регистрационных карточек от руки чернилами или пастой. Фамилии, имена, отчества физических лиц, наименования юридических лиц, обстоятельства совершения правонарушения записываются печатными буквами.

В регистрационных карточках не допускаются исправления. Вносимые сведения должны точно отражать содержание принятых процессуальных решений, строго соответствовать установленным в порядке, предусмотренном законодательными актами, фактам и событиям и подтверждаться материалами дела.

### Порядок фиксации сведений об административном правонарушении

Если постановление о наложении административного взыскания вынесено должностным лицом регистрирующего органа, фиксация сведений об административном правонарушении осуществляется регистрирующим органом непосредственно в банке данных регистрационной информации о правонарушениях (без заполнения регистрационной карточки на бумажном носителе информации), а также в журнале регистрации административных правонарушений не позднее трех суток после:

- вступления в законную силу постановления о наложении административного взыскания;
- если постановление по делу об административном правонарушении было обжаловано (опротестовано) до вступления в законную силу после возвращения дела из суда, органа (от должностного лица), рассмотревшего жалобу (протест), за исключением случая, если по жалобе (протесту) вынесено постановление в соответствии с пунктами 2, 3, 6 или 7 части 1 статьи 12.9 данного Кодекса;
- вынесения постановления о наложении административного взыскания в соответствии с частью 1 статьи 10.3 Процессуально-исполнительного кодекса Республики Беларусь об административных правонарушениях;
- получения сведений об уплате штрафа физическим лицом, в отношении которого вынесено постановление о наложении административного взыскания в соответствии с частью 3 статьи 10.3 Процессуально-исполнительного кодекса Республики Беларусь об административных правонарушениях.

Регистрационная карточка формы 1-АП не заполняется в случае, если невозможно установить достоверные сведения о физическом лице, привлеченном к административной ответственности в соответствии:

- с частью 1 статьи 10.3 Процессуально-исполнительного кодекса Республики Беларусь об административных правонарушениях;
- с частью 3 статьи 10.3 Процессуально-исполнительного кодекса Республики Беларусь, если штраф в размере до двух базовых величин уплачен на месте.

Если дело об административном правонарушении подлежит передаче для рассмотрения в другой орган, ведущий административный процесс, или суд, регистрирующий орган в сроки, предусмотренные статьей 10.30 Республики Процессуально-исполнительного кодекса Беларусь об административных правонарушениях, фиксирует установленные ДО рассмотрения сведения об административном правонарушении, дела совершенном физическим лицом, в регистрационной карточке формы 1-АП, об административном правонарушении, совершенном юридическим лицом, в регистрационной карточке формы 3-АП. Допускается фиксация сведений об административном правонарушении непосредственно в банке данных информации регистрационной 0 правонарушениях cпоследующей распечаткой соответствующей регистрационной карточки.

Регистрационная карточка формы 1-АП (3-АП) подписывается уполномоченным работником регистрирующего органа и направляется в другой орган, ведущий административный процесс, или суд вместе с делом об административном правонарушении.

#### Порядок фиксации сведений о преступлении

Фиксация сведений о преступлении в соответствующих регистрационных карточках следователем, дознавателем осуществляется, как правило, не позднее суток после вынесения соответствующих постановлений.

## Порядок учета правонарушений и представления сведений о правонарушениях органами внутренних дел

Учет правонарушений осуществляют информационно-аналитические подразделения органов внутренних дел.

Первичный учет правонарушений осуществляется путем заполнения документов первичного учета (статистических карточек).

#### Общая схема функционирования ЕГСРУП:

1. В каждом органе уголовного преследования, органе, ведущем административный процесс, суде, органе, осуществляющем исполнение наказания, в целях сосредоточения совокупности сведений о зарегистрированных ими правонарушениях создается специализированная информационно-техническая система — банк данных регистрационной информации о правонарушениях.

Помещение сведений в банк данных регистрационной информации осуществляется:

- об административном правонарушении не позднее трех суток после вынесения постановления о наложении административного взыскания.
- о преступлении не позднее суток после заполнения следователем, либо дознавателем регистрационных карточек. Допускается фиксация сведений о правонарушениях следователем, дознавателем непосредственно в банке данных регистрационной информации о правонарушениях с последующей распечаткой регистрационных карточек на бумажных носителях.
- 2. Сведения о правонарушениях, помещенные в банк данных регистрационной информации о правонарушениях, по техническим каналам передачи данных либо на магнитных (электронных) носителях информации ежедневно по рабочим дням передаются регистрирующими органами в информационные подразделения управлений, отделов внутренних дел в городах, районах, районах в городах и на транспорте.
- 3. Поступившие в учетное подразделение из регистрирующего органа по электронным каналам сведения об административных правонарушениях не позднее суток после их поступления помещаются в территориальный банк данных о правонарушениях информационно-техническую систему, находящуюся в ведении управлений, отделов внутренних дел в городах, районах, районах в городах и на транспорте и включающая совокупность сведений о правонарушениях, зарегистрированных соответственно в городах, районах, районах в городах и на объектах транспорта.

Помещенные в территориальный банк данных о правонарушениях сведения об административных правонарушениях ежедневно передаются учетным подразделением по электронным каналам в информационно-аналитические подразделения ГУВД, УВД, УВДТ по подчиненности.

правонарушениях, поступившие Сведения об ИЗ подразделений, не позднее суток после их поступления помещаются информационно-аналитическими подразделениями ГУВД, УВД, УВДТ в региональный банк данных о правонарушениях — информационнотехническую систему, находящуюся В ведении ГУВД горисполкома, УВД облисполкомов, УВДТ и включающая совокупность о правонарушениях, зарегистрированных соответственно г. Минске, областях и на транспорте.

Помещенные в региональный банк данных о правонарушениях сведения об административных правонарушениях ежедневно передаются информационными подразделениями ГУВД, УВД, УВДТ по электронным каналам в информационный центр МВД.

5. Сведения об административных правонарушениях, поступившие из информационных подразделений ГУВД, УВД, УВДТ, помещаются информационным подразделением МВД в единый государственный банк данных о правонарушениях не позднее суток после их поступления.

Сведения о преступлениях, помещенные в единый государственный банк данных о правонарушениях, хранятся сто лет. Сведения об

административных правонарушениях, помещенные в единый государственный банк данных о правонарушениях, хранятся десять лет.

# 3. Особенности получения информации в автоматизированных банках данных МВД

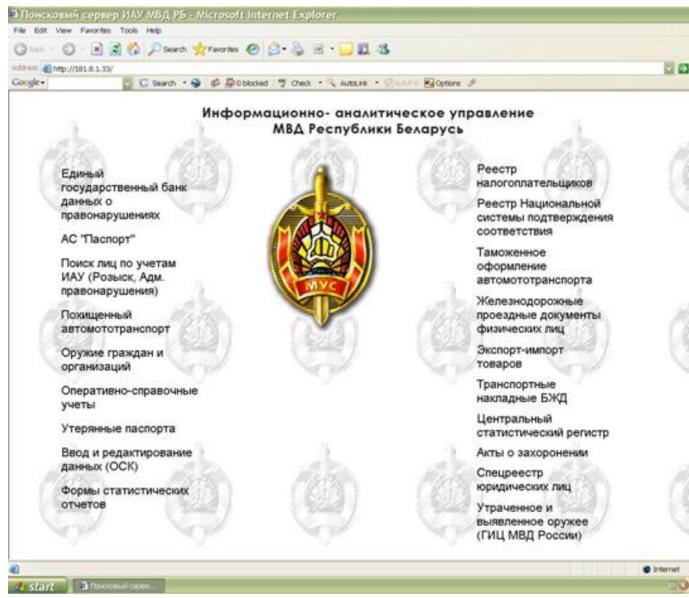
#### 3.1. Информационно-поисковый сервер

#### информационно-аналитического управления МВД Республики Беларусь

На сегодняшний день в условиях широкой компьютеризации и информатизации органов внутренних дел преобладающей формой работы с информацией, сосредоточенной в различного вида учетах, становятся автоматизированные информационные поисковые системы и автоматизированные банки данных.

Отличительной особенностью является то, что реализация единой информационной сети органов внутренних дел позволяет сотруднику оперативно получать интересующую информацию из ряда автоматизированных банков данных напрямую.

С этой целью в 2004 году в Информационно-аналитическом управлении МВД Республики Беларусь (сейчас информационный центр) был создан информационно-поисковый сервер.



Технической основой работы данного сервера являются интернеттехнологии.

Организационно доступ к информационным ресурсам сервера ИАУ МВД Республики Беларусь осуществляется по мотивированному рапорту в порядке, рассмотренном ранее во втором вопросе данной лекции.

Реквизитный состав баз данных информационно-поискового сервера ИЦ МВД Республики Беларусь включает в себя различную информацию. На примере некоторых автоматизированных информационных поисковых систем, рассмотрим их основные информационные возможности, что позволит в будущем целенаправленно осуществлять поиск необходимой информации.

### 3.2. Назначение, реквизитный состав и порядок подключения к AC «Паспорт»

АС «Паспорт» предназначена для:

• сбора и хранения информации, содержащейся в заявлениях формы 1 на получение паспортов гражданами Республики Беларусь, вида на

- жительство иностранными гражданами и лицами без гражданства в Республике Беларусь и проездных документов Республики Беларусь;
- обеспечения оперативного поиска и получения информации о гражданах Республики Беларусь, иностранных гражданах и лицах без гражданства в целях своевременного предупреждения, выявления и расследования правонарушений;
- предотвращения использования недействительных документов в противоправных целях. (рис. см. на слайде)

Реквизитный состав автоматизированной системы «Паспорт»:

- личный номер;
- фамилия, имя, отчество;
- пол, дата рождения;
- место рождения: страна, область, район, населенный пункт;
- семейное положение, фамилия, имя, отчество супруга, дата рождения супруга, наименование органа загса, дата регистрация брака;
- сведения о детях: фамилия, имя, отчество, дата рождения, пол;
- родители: фамилия, имя, отчество, степень родства;
- причина выдачи паспорта;
- нахождение в иностранном гражданстве, вид документа, серия документа, номер документа, наименование учреждения, выдавшего документ, дата выдачи документа;
- номер и серия паспорта; кем выдан паспорт (наименование ОВД); дата выдачи паспорта; срок действия паспорта;
- место жительства при получении паспорта; страна, область, район, населенный пункт, улица, дом, корпус, квартира;
- орган, выдавший разрешение на выезд за границу; дата принятия решения; срок действия разрешения.

Удаленный доступ к AC «Паспорт» предоставляется по рапорту начальников подразделений центрального аппарата И центрального подчинения Министерства внутренних дел Республики Беларусь, главного управления внутренних дел Минского городского исполнительного комитета, управлений внутренних дел областных исполнительных комитетов, управления внутренних дел на транспорте на имя заместителя Министра внутренних дел — начальника главного управления милиции общественной безопасности и специальной милиции.

В рапорте указываются:

- обоснование необходимости получения информации из АС «Паспорт»;
- категория запрашиваемой информации;
- фамилия, имя, отчество, должность и специальное звание сотрудника, ответственного за использование и получение информации АС «Паспорт» и номер его служебного телефона;
- IP-адрес компьютера, с которого будет осуществляться вход в AC «Паспорт».

При положительном решении вопроса о предоставлении удаленного доступа сотруднику, ответственному за использование AC «Паспорт», сообщается имя и пароль доступа для входа в AC «Паспорт».

Удаленный доступ к AC «Паспорт» предоставляется сроком на один год. Для продления срока удаленного доступа к AC «Паспорт» повторно подается рапорт в порядке, установленном Инструкцией.

- В соответствии с Инструкцией техническими средствами обеспечивается ведение и хранение протокола пользования сведениями, хранящимися в АС «Паспорт». При этом СОТРУДНИК, ОТВЕТСТВЕННЫЙ ЗА ИСПОЛЬЗОВАНИЕ АС «ПАСПОРТ», ОБЯЗАН:
- использовать удаленный доступ к AC «Паспорт» только в служебных целях;
- не допускать передачи другим лицам имени и пароля доступа в AC «Паспорт»;
- не допускать распространения (разглашения) персональных данных граждан, хранящихся в АС «Паспорт».

При увольнении или переводе сотрудника, получившего удаленный доступ к АС «Паспорт», в соответствии с Инструкцией начальник органа внутренних дел в трехдневный срок направляет об этом сообщение в бюро паспортизации населения Министерства внутренних дел Республики Беларусь.

#### 3.3. Назначение, реквизитный состав и порядок подключения к АИС «ГАИ-ЦЕНТР»

АИС «ГАИ-Центр» предназначена для повышения эффективности использования централизованных оперативно-справочных, розыскных и криминалистических учетов, обеспечения единой технической политики в области создания и внедрения информационных систем подразделениями ГАИ Министерства внутренних дел.

Работа в АС «ГАИ-центр» доступна по следующим разделам:

- учет водительских удостоверений;
- утраченные водительские документы;
- регистрация авто,-мото транспорта;
- лишение водительского удостоверения;
- розыск авто,-мото транспорта;
- розыск лиц по дорожно-транспортным происшествиям;
- учет дорожно-транспортных происшествий;
- нарушение Правил дорожного движения;
- общий поиск.

Удаленный доступ к АИС «ГАИ-Центр» предоставляется подразделениям органов внутренних дел, а также государственным органам для получения информации по следующим категориям:

• зарегистрированные транспортные средства и транспортные средства, находящиеся в залоге или под арестом;

- выданные водительские удостоверения и лица, лишенные права управления транспортными средствами;
- дорожно-транспортные происшествия.

Удаленный доступ подразделениям органов внутренних дел к АИС «ГАИ-Центр» предоставляется по рапорту начальников подразделений центрального аппарата и центрального подчинения Министерства внутренних дел Республики Беларусь, начальника главного управления внутренних дел Минского городского исполнительного комитета, начальников управлений внутренних дел областных исполнительных комитетов, управления внутренних дел на транспорте Министерства внутренних дел Республики Беларусь, а также их заместителей на имя заместителя Министра внутренних дел — начальника главного управления милиции общественной безопасности.

В рапорте указываются:

- обоснование необходимости предоставления информации из АИС «ГАИ-Центр»;
- категория запрашиваемой информации;
- фамилия, имя, отчество, должность и специальное звание сотрудника, ответственного за получение информации из АИС «ГАИ-Центр», номер его служебного телефона;
- IP-адрес компьютера, с которого будет осуществляться вход в АИС «ГАИ-Центр».

При положительном решении вопроса о предоставлении удаленного доступа сотруднику, ответственному за получение информации из АИС «ГАИ-Центр», сообщается имя и пароль доступа. Срок действия доступа — один год.

Предоставление удаленного доступа к АИС «ГАИ-Центр» осуществляется Центром информационных технологий управления связи и автоматизации Департамента финансов и тыла МВД (по согласованию с управлением Государственной автомобильной инспекции Министерства внутренних дел Республики Беларусь. (рис. см. на слайде)

Реквизитный состав базы данных:

по автотранспортным средствам

- серия и номер технического паспорта автотранспортного средства,
- марка, модель, модификация, год выпуска, номер двигателя, номер кузова, номер шасси, цвет, номерной знак.
- фамилия, имя, отчество, дата и место рождения, место жительства владельца.
- дата выдачи технического паспорта автотранспортного средства.
- особые отметки;

по дорожно-транспортным происшествиям

- год, область, номер ДТП.
- дата, время ДТП (час, минута).
- погибло, ранено, ущерб.

- категория ДТП, код места совершения ДТП.
- дорога, погодные условия.

ВРЕМЯ ПОСТУПЛЕНИЯ ИНФОРМАЦИИ В УВД

- даты составления, изменения и отправки карточки;
- фамилия, имя, отчество, дата рождения, номер и серия паспорта, место прописки и место жительства гражданина, место работы, род занятий.
- статья КоАП, дата совершения административного правонарушения.

Результаты поиска похищенного АМТ выводятся в виде карточки: № ЦИАУ 5947532 № ГИЦ 9028515 вид операции ПОСТАВЛЕНА НА УЧЕТ TMA DNT BA321150 **МАРКА/МОДЕЛЬ** ЦВЕТ НЕ УКАЗАН НОМЕРНОЙ ЗНАК 144AE0116 2007 ГОД ВЫПУСКА XTA21150074312846 НОМЕР КУЗОВА НОМЕР ШАССИ 4504410 номер двигателя НОМЕР РАМЫ 1192 ТАТАРСКАЯ АССР РЕГИОН ПОСТАНОВКИ ПРИЧИНА ПОСТАНОВКИ 05.04.2007 дата постановки 03.04.2007 дата хищения 00:00 вид документа ДОКУМЕНТ № 03.04.2007 464738 дата документа место хищения НОВО-САВИНОВСКОЕ КОММЕНТАРИЙ владелец HOMEP ТЕХПАСПОРТ СЕРИЯ ВРЕМЯ ПОСТУПЛЕНИЯ ИНФОРМАЦИИ ОТ ЗАЯВИТЕЛЯ ВРЕМЯ ОБРАБОТКИ ИНФОРМАЦИИ СОГ

### 3.4. Назначение, реквизитный состав и порядок подключения АИС «ФР-ОПОВЕЩЕНИЕ»

Железнодорожные проездные документы физических лиц

Фамилия	
	□Поиск по фонеме
Серия документа	
Номер документа	
Дата покупки	
Дата отправления	
Станция	
отправления	
Станция назначения	
Номер поезда	The Part of the Pa
Номер вагона	
Номер места	

Информация о лицах, которые приобрели ж.д. билеты на поезда, следующие на территори Украины и Молдовы, накапливается в УВДТ - с 01 апреля 1999 г., в страны Балтии - с 1 ав на территорию Республики Беларусь с России - с 1 декабря 2006 г.

#### Реквизитный состав:

- фамилия, имя, отчество.
- паспортные данные (серия, номер).
- дата приобретения билета.
- дата отправления.
- станции отправления и назначения.
- номер поезда, номер вагона, номер места.
  - 3.5. Назначение, реквизитный состав и порядок подключения **АИС** «Оружие граждан и организаций»

	АИС '	'ОРУЖИЕ''	
Фамилия			
кмИ			
Отчество			
Организация			
Марка/модель			
Серия		Калибр	
Номер		Кол-во стволов	
Год выпуска			
Сортировка	⊙По оружию ⊙По владельцу		
	Поиск	Очистить	

Реквизитный состав базы данных:

- фамилия, имя, отчество.
- дата рождения.
- паспорт, идентификатор нового паспорта.
- место рождения и жительства гражданина.
- наименование и адрес организации, учреждения или предприятия.
- вид оружия, изготовитель, марка-модель, серия, номер, калибр, год выпуска, количество стволов, производство, назначение.
- право владения, сроки разрешения на оружие.
- шифр РОВД, дата загрузки в базу.

		Pes	ультат поис	ка	
		Вла	делец		
(			ОВСКИЙ ВО	ОДИТЕЛЬ ИВАН ХНДРОВИЧ	ОВ
Дата рождения		Паспорт	0000000000	Идентификатор	)
				район ТУЛЬС	СИЙ
рождения н					
11/10/07/07/10 10 14			СКИЙ ЖАБИ		
жительства	л.КОЛХО	ЗНАЯ д	.0000 кор.0	00 кв.0000	
Op	ужие: 00	0000000	00000000000	000000000	
Вид оружия	РУЖЬЕ			Назначение	ОХОТНИЧЬЕ
Серия	00000	Номер	0000000000	Право владения	личное
Год выпуска	0000	Калибр (мм.)	12	Изготовитель	ТУЛЬСКИЙ 3-Д
Кол-во стволов	0				
Разрешение №	00000000	Дата выдачи		Сроком до	

3.6. Назначение, реквизитный состав и порядок подключения **AC** «Единый реестр налогоплательщиков Республики Беларусь»

### РЕЕСТР НАЛОГОПЛАТЕЛЬЩИКОВ

	HANMEH	OBAHNE		
полное				
краткое				
	PEKB	изиты		
унн	номер счета		код банка	
	АД	PEC		
город		улица 📗		
	РУКОВО	ДИТЕЛЬ		
фамилия	RMN		отчество	
	БУХГ	АЛТЕР		
фамилия	RMN		отчество	
	УЧРЕД	ИТЕЛЬ		
наименование				
паспорт				

Реквизитный состав:

- универсальный № налогоплательщика,
- учредитель.
- название и адрес фирмы.
- банк и № расчетного счета.
- ФИО руководителя и главного бухгалтера.

• дата регистрации.

Результаты поиска конкретного юридического лица выводятся в виде карточки:

ıμι	очки.
	налогоплательщин
	унн <b>100012665</b>
	Код ГНИ ИМНС по Заводскому р-ну г. Минска
	Полное наименование МАЛОЕ НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ "ОПТИКОР"
	Краткое наименование <b>МП"ОПТИКОР"</b>
	Адрес 220137, Г.МИНСК, УЛ.АНГАРСКАЯ,71
	Форма собственности Собственность негосударственных юридических лиц
	Вышестоящий орган ЮРИДИЧЕСКИЕ ЛИЦА БЕЗ ВЕДОМСТВЕННОЙ ПОДЧИНЕННОСТИ
	Статус Юридическое лицо
	Вид налогоплательщика <b>Другие коммерческие предприятия</b>
	Руководитель <b>ИВАНОВ ВЛАДИСЛАВ НИКОЛАЕВИЧ</b>
	Телефон 80172-489174
	Бухгалтер ИВАНОВ ВЛАДИСЛАВ НИКОЛАЕВИЧ
	Телефон
	Вид деятельности ИССЛЕДОВАНИЯ И РАЗРАБОТКИ
	Регистрирующий орган <b>Райисполком</b>
	Дата регистрации 27-NOV-90
	Номер регистрации 155
	Дата корректировки 22-MAR-04
	Признак резидента СЭЗ
	счета
Iет	счетов
	учредители
	Учредитель <b>ИВАНОВ ВЛАДИСЛАВ НИКОЛАЕВИЧ</b>
	Aggec 220000 F,MiHCK TP.POKOCCOBCKOFO,113,KB.38
	Паспорт У-ВН,514603,01.01.1990,ЛЕНИНСКИМ РОВД Г.МИНСКА
	УНН учредителя
	Статус Гражданин РБ (физическое лицо)
П	ризнак резидента <b>резидент</b>
	га корректировки 18-FEB-02

# 3.7. Назначение, реквизитный состав и порядок подключения **AUC** «Таможенное оформление **AMT**»

	Лицо	
Фамилия		
<b>И</b> МЯ		
Отчество		
Номер и серия паспорта		
	Автомобиль	
паспорта	Автомобиль	
	Автомобиль	

Реквизитный состав:

- фамилия, имя, отчество.
- дата рождения.

- паспорт.
- место жительства гражданина.
- вид AMT.
- марка АМТ, номер кузова, номер двигателя.
- дата оформления.
- таможенный режим.

Карточка результатов поиска выглядит следующим образом:

Владелец ИВАНОВ СЕРГЕЙ АРКАДЬЕВИЧ

Паспорт АВ 0199567 выдан 08.04.1998 РОВД ЛЯХОВИЧИ

Страна гражданства РЕСПУБЛИКА БЕЛАРУСЬ

Область РБ

Район РБ

Наименование города ЛЯХОВИЧСКИЙ РН. Д.ЗАЛИПЕНЬЕ

Адрес ул. дом корп. кв.

Вид АМТС ЛЕГКОВОЙ
Марка АМТС ALFA ROMEO

Модель 930

Дата выпуска 30.06.1997

Номер кузова ZAR9300004118718

Номер шасси

Номер двигателя

Дата оформления 12.10.2004

Таможня "ЗАПАДНЫЙ БУГ"

Таможенный режим ВЫПУСК В СВОБОДНОЕ ОБРАЩЕНИЕ

Номер удостоверения ТС-25а

### 3.8. Назначение, реквизитный состав и порядок подключения AC «Спецреестр юридических лиц»

<u>Н</u> аименование	5
<u>y</u> hh	100
<u>С</u> чет(а)	
Учредитель, физ. или юр	. лицо:
Фамилия(наименование)	
Имя	
Отчество	
Руководитель:	
Фамилия	
Имя	
Отчество	
Бухгалтер:	
Фамилия	
Имя	
Отчество	

#### Реквизитный состав:

- универсальный № налогоплательщика,
- учредитель.
- название и адрес фирмы.
- банк и № расчетного счета.
- ФИО руководителя и главного бухгалтера.
- дата регистрации.

Результаты поиска содержат помимо установочных данных юридического лица, так же информацию, касающуюся фактов незаконной деятельности.

Наименование	000 "СЕРЕБРЯННЫЙ БОР"
Адрес	Г. МИНСК УЛ. ПЛЕХАНОВА, 63-103
Регистрирующий орган	Райисполком
Дата регистрации	22.04.1997
Номер регистрации	17746
УНН	100031514
Используемые счета	3012006430017 (Минск. Филиал 0101 ЗАО "Минский транзитный банк");
Руководитель	ИВАНОВ ИГОРЬ АЛЕКСАНДРОВИЧ, ПР-Н Г. МИНСК, УЛ. ГАМАРНИКА,9-1-33, П-Т ∨ ВН №615137, ВЫДАН ОВД ФРУНЗЕНСКОГО РИК Г.МИНСКА 30.01.1979Г.
Бухгалтер	отсутствует
Информация об учредителях	ДАВИСКИБА АЛЕКСЕЙ ИВАНОВИЧ (11-ВН № 674712, ВЫДАН ОВД ЛЕНИНСКОГО РИК Г. МИНСКА 25.06.1977Г.);
	малышева тамара андреевна (MP 1188857, 03,12,01, ЦЕНТРАЛ РОВД Г.МИНСКА);
Состоит на учете	ИМНС по Ленинскому р-ну г. Минска
Проводило проверку	ИМНС по Ленинскому р-ну г. Минска
Иной орган проводивший проверку	
Дата последней проверки, которая имеет косвенные либо прямые признаки указывающие на лжепредпринимательство	16.01.2000
Всего (сумма налогов, сборов, иных платежей и экономический санкций, допричисленных по результатам последней проверки), млн. руб.	16,88
Дата направления материалов в правоохранительные органы	11.11.2000
Результат рассмотрения в правоохранительных органах	ОТКАЗАНО В ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА
Период деятельности в качеств	е лжепредпринимательской структуры:
начало	22.04.1997
конец	31.12.1999
Дата направления ходотайства о ликвидации	02.10.2003
Результат рассмотрения ходотайства	в стадии ликвидации
Дата приостановления	26.05.2000

### 3.9. Другие автоматизированные информационно-поисковые системы

Кроме указанных выше в ИАУ МВД Республики Беларусь сотрудникам органов внутренних дел доступны ряд автоматизированных информационных систем.

## Автоматизированная информационно-поисковая система «Профилактируемые лица»

НАИМЕНОВАНИЕ БАЗЫ ДАННЫХ: учет профилактируемого контингента.

РЕКВИЗИТНЫЙ СОСТАВ БАЗЫ ДАННЫХ:

- шифр РОВД.
- фамилия, имя, отчество.
- дата рождения.
- паспорт, идентификатор нового паспорта.

- место рождения и жительства гражданина.
- место работы.
- клички.
- категория учета.
- интересы, имеет навыки.
- ранее судим по статьям, количество судимостей.
- вид дела-материала, номер и дата заведения дела-материала,
- линия работы.
- связи лица.
- пол, рост, внешне похож, телосложение, волосы, особенности поведения, особые приметы и татуировки.
- дата загрузки в базу.

## Автоматизированная информационно-поисковая система «Профилактируемые лица»

НАИМЕНОВАНИЕ БАЗЫ ДАННЫХ: учет утраченных (похищенных, утерянных) и выявленных (изъятых, найденных, добровольно сданных) номерных вещей.

### РЕКВИЗИТНЫЙ СОСТАВ БАЗЫ ДАННЫХ:

- шифр РОВД.
- серия, номер, код вещевой группы.
- наименование, принадлежность.
- причина заполнения документа.
- марка-модель.
- количество, форма, фасон, тип, размер, калибр, инвентарный номер.
- место хищения (изъятия).
- детали (марка, серия, номер).

## Автоматизированная информационно-поисковая система «АБД-розыск»

НАИМЕНОВАНИЕ БАЗЫ ДАННЫХ: учет неопознанных трупов, без вести пропавших, больных.

### РЕКВИЗИТНЫЙ СОСТАВ БАЗЫ ДАННЫХ:

- категория учета.
- дактоформула.
- формула учета.
- дата исчезновения-обнаружения.
- возраст.
- фамилия, имя, отчество.
- дата рождения.
- место рождения, жительства, работы гражданина.
- описание примет.
- шифр РОВД.
- номер и дата заведения дела.

# Автоматизированная информационно-поисковая система «Республиканский розыск»

НАИМЕНОВАНИЕ БАЗЫ ДАННЫХ: учет лиц, объявленных в республиканский розыск.

### РЕКВИЗИТНЫЙ СОСТАВ БАЗЫ ДАННЫХ:

- фамилия, имя, отчество.
- дата рождения.
- паспортные данные.
- место рождения и жительства гражданина.
- поп
- национальность.
- дактоформула.
- причина розыска.
- вид преступления.
- мера пресечения.
- уголовное дело, розыскное дело.
- шифр РОВД.
- информация на должника-алиментщика.
- дата загрузки в базу.

## Автоматизированная информационно-поисковая система «Учет неопознанных трупов»

НАИМЕНОВАНИЕ БАЗЫ ДАННЫХ: учет неопознанных трупов. РЕКВИЗИТНЫЙ СОСТАВ БАЗЫ ДАННЫХ:

- пол.
- дата обнаружения.
- номер и дата заведения дела оперативной проверки (ДОП),
- шифр РОВД.
- дата прекращения и причина прекращения ДОП.
- дата загрузки в базу.

# Автоматизированная информационно-поисковая система «Коммерческие предприятия, занимающиеся незаконным вывозом товаров из Республики Беларусь»

НАИМЕНОВАНИЕ: республиканская база данных коммерческих предприятий, занимающихся незаконным вывозом товаров из республики.

### РЕКВИЗИТНЫЙ СОСТАВ БАЗЫ ДАННЫХ:

- наименование органа.
- шифр органа.
- наименование предприятия.
- дата регистрации.
- форма собственности и адрес.
- руководитель.
- учредитель.
- какой товар вывозился.

- какой транспорт использовался.
- принятые меры.
- дата.

## Автоматизированный учет ввозимых и вывозимых грузов субъектами хозяйствования Республики Беларусь.

НАИМЕНОВАНИЕ: учет грузовых таможенных деклараций. РЕКВИЗИТНЫЙ СОСТАВ БАЗЫ:

- номер грузовой таможенной декларации (ГТД),
- код получателя.
- адрес получателя, наименования получателя,
- код контрактодержателя и его адрес.
- учетный номер налогоплательщека заявителя.
- наименование и адрес заявителя.
- код товара.
- наименование товара.
- маркировка товара, вес, стоимость в валюте.
- дата оформления ГТД и адрес таможни.
- дата контракта, номер контракта.
- наименование и адрес отправителя.

#### БД АСПК «Пассажиропоток»

В соответствии с установленным порядком удаленный доступ к информации, содержащейся в БД автоматизированной системы пограничного контроля о гражданах Республики Беларусь, иностранных гражданах и лицах без гражданства, пересекающих Государственную границу Республики Беларусь (БД АСПК «Пассажиропоток») предоставляется информационным центром МВД Республики Беларусь органам внутренних дел, зарегистрированным в компьютерной сети МВД Республики Беларусь.

Удаленный доступ к информации, содержащейся в БД АСПК «Пассажиропоток» предоставляется по рапорту начальников подразделений центрального аппарата и центрального подчинения МВД, ГУВД Мингорисполкома, УВД областей, УВДТ на имя заместителя Министра внутренних дел Республики Беларусь — начальника милиции общественной безопасности.

В рапорте указывается:

- основание необходимости получения удаленного доступа к БД АСПК «Пассажиропоток»;
- фамилия, имя, отчество должность и специальное звание сотрудника, ответственного за получение и использование информации БД АСПК «Пассажиропоток», номер его служебного телефона;
- IP-адрес компьютера, с которого будет осуществляться вход в БД АСПК «Пассажиропоток».

Удаленный доступ к БД АСПК «Пассажиропоток» предоставляется сроком на один год.

ПЕРЕЧЕНЬ ДАННЫХ, ПРЕДОСТАВЛЯЕМЫХ ОРГАНАМ ВНУТРЕННИХ ДЕЛ ИЗ БД АСПК «ПАССАЖИРОПОТОК».

- фамилия;
- имя;
- дата рождения;
- пол;
- личный номер (для граждан РБ);
- тип документа;
- гражданство лица, пересекающего Государственную границу Республики Беларусь;
- номер предъявленного документа на пересечение Государственной границы Республики Беларусь;
- пункт пропуска через Государственную границу Республики Беларусь, через который гражданин пересек Государственную границу Республики Беларусь;
- дата и время пересечения Государственной границы Республики Беларусь.

Таким образом, к настоящему времени в органах внутренних дел накоплен определенный опыт автоматизированной обработки информации оперативно-розыскных, оперативно-справочных И криминалистических учетно-регистрационных И аналитико-статистических данных уголовной преступности, сведений управленческого, плановоэкономического, финансового характера, а также данных по отдельным специализированным направлениям деятельности служб и подразделений. И от того, насколько успешно будущий работник правоохранительных органов овладеет основами работы с автоматизированными банками данных, используемых в практической деятельности в органах внутренних дел, во многом будет завысить его последующая профессиональная деятельность.