Материал для самостоятельного изучения по дисциплине «Информационные системы в профессиональной деятельности»

Лекция № 7

Тема 2.4. Технология использования систем управления базами данных

Урок № 20

Количество часов: 2

Цель: Сформировать знания у студентов о системе управления базами данных.

План лекции:

1. Необходимость баз данных.
2. Понятие базы данных.
3. Классификация баз данных.
4. Общая характеристика СУБД MS Access.
    - 4.1. Таблицы.
    - 4.2. Запросы.
    - 4.3. Формы.
    - 4.4. Отчеты.
    - 4.5. Макросы и модули.
    - 4.6. Связь между таблицами и целостность данных.
    - 4.7. Сервисные операции.
5. Тестовые задания для самопроверки.

1. Необходимость баз данных

Большая часть публикуемой информации представлена также в удобном формате в виде компьютерных баз данных, предназначенных для распространения в электронном виде. В 1980-90 годы количество баз данных, равно как и их поставщиков, резко возросло. Компьютерные базы данных имеют ряд преимуществ по сравнению с печатными материалами.

Благодаря использованию компьютеров как основополагающего звена технологии сбора и обработки информации, предоставляемые данные являются самыми "свежими", актуальными.

Процесс поиска данных отличается доступностью, быстротой и простотой. Предоставляется возможность доступа к сотням наименований баз данных. При этом обеспечивается практически мгновенный доступ к требуемой информации благодаря упрощенному процессу поиска, для которого используются стандартные, одинаковые у всех поставщиков поисковые протоколы и команды.

Благодаря высокой скорости передачи информации плата за доступ к компьютерным базам данных относительно небольшая.

Пользование базами данных очень удобно и может осуществляться посредством персонального компьютера с подключенным к нему соответствующим устройством связи, как, например, модем или коммуникационная сеть.

Необходимо отметить, что компьютерные базы данных охватывают огромнейшие объемы разнообразной информации, в которой можно легко запутаться. Поэтому целесообразной представляется классификация компьютерных баз данных.

2. Понятие базы данных

В современных информационно-вычислительных системах (ИВС) одной из центральных является функция хранения, обработки и представления пользователям информации. Примерами таких ИВС являются банковские ИВС, ИВС резервирования билетов, мест в гостиницах. Для хранения информации в ИВС, как правило, используют базу данных.

Для управления базами данных, их создания и ведения используются специализированные программные комплексы **системы управления базами данных** (**СУБД**). Их основные **функции**:

- Создание информационных структур для хранения информации.
- Реализация запросов, удовлетворяющих определенным требованиям.
- Создание отчетов с возможным анализом информации БД.
- Разработка форм, как электронных аналогов бумажных документов.

- Программирование задач пользователя по работе с БД.
- Реализация многопользовательского доступа к БД.
- Защита информации в БД с помощью паролей, шифрации и др.

База данных - совокупность структурированных данных, относящихся к определенной предметной области. Хорошо спроектированная база данных содержит совокупность не избыточных не противоречащих данных, защищенных от несанкционированного доступа. Пользователями базы данных могут быть различные прикладные программы, программ комплексы, специалисты предметной области, выступающие в роли потребителей или источника трансформации. Для управления базой данных служит система управления базами данных или сокращенно СУБД, т.е комплекс программных языковых средств, необходимых для создания баз данных, поддержание их в актуальном состоянии и организация поиска в них необходимой информации.

Структурные элементы базы данных:

1. *Поле* – это элементарная единица логической организации данных, которая соответствует отдельной неделимой единице информации, т.е. реквизиту.
2. *Реквизит* – логический идеальный информационный элемент, описывающий определенные особенности объекта, процесса или явления.
3. *Запись* – совокупность логически связанных полей.
4. *Файл* – совокупность одинаковых по структуре экземпляров записей. Каждый экземпляр записи однозначно идентифицирует уникальным ключом записей.

Назначение баз данных: для решения сложных научных, экономических и производств задач применяются системы искусственного интеллекта. Представление знаний и разработка систем, основанных на знаниях – это одно из направлений искусственного интеллекта. Знание – это выявление закономерностей предметной области, т.е принципы, связи и законы, которые позволяют решать задачи в этой области.

3. Классификация компьютерных баз данных

Компьютерные базы данных делятся на базы данных с доступом в режиме online, offline и через Internet. Базы данных с доступом в режиме online (online databases) хранятся в центральном банке данных. Доступ к ним осуществляется посредством компьютера (или иного терминала) через телекоммуникационную сеть. Доступ, поиск и анализ Internet - баз данных (internet databases) осуществляется посредством Internet. Сведения из них можно загружать и сохранять на компьютере или вспомогательном запоминающем устройстве. Базы данных с доступом в режиме offline (offline databases) представляют собой информацию, хранящуюся на дискетах или компакт-дисках и доступную для потребителей без использования внешней телекоммуникационной сети.

Описанные виды баз данных в свою очередь подразделяются на библиографические, цифровые, текстовые, справочные и специализированные.

Библиографические базы данных (bibliographic databases) состоят из ссылок и цитат из статей журналов, газет, отчетной документации маркетинговых исследований, технических докладов, правительственной документации и т.п. Они часто содержат краткие изложения и отрывки из цитируемых материалов. Примерами библиографических баз данных могут бытьABI/Infonm терминальная система Predicasls. Библиографическая база данных Management Contents, предлагаемая компанией Dialog Corporation, использовалась в проекте «Выбор универмага» при поиске необходимой литературы.

Цифровые базы данных (numeric databases) содержат цифровую и статистическую информацию. Например, некоторые цифровые базы данных

предоставляют хронологически систематизированную информацию о структуре и специфической продукции ряда компаний - это Boeing Computer Services Co., Data Resources, Evans Economics и Министерство управления и развития экономики. Существуют также цифровые базы данных, которые используют информацию переписей населения и жилья 1980 и 1990 годов и предоставляют обновленные данные, систематизированные в соответствии с кодом переписи и почтовым индексом. Поставщиками таких баз данных являются Бюро переписей США, Donnelly Marketing Information Services, CACI, Inc. и National Decision System.

Текстовые базы данных (full-text databases) состоят из полных текстов оригинальных документов. Один из крупнейших поставщиков баз данных этого типа - компания Vu/Text Information Systems, Inc., которая предоставляет услуги по рассылке полных текстов в электронном виде, а также предоставляет возможность поиска информации из множества газет (например, Washington Post, Boston Globe, Miami Herald). Компания Mead Data Centralпредлагает потребителям услугу N EXIS. которая предполагает возможность доступа к полным текстам сотен коммерческих баз данных, включающих избранные газеты, периодические издания, годовые отчеты компаний и инвестиционных фирм.

4. Основы работы СУБД MS ACCESS

Рассмотрим работу СУБД на примере MS Access, входящей в профессиональный пакет MS Office.

В начале работы с Access происходит создание новой базы данных с присвоением файлу базы оригинального имени и расширения .mdb.

В каждой базе данных имеется окно базы. В этом окне находится панель *Объекты* с кнопками *Таблицы, Запросы, Формы, Отчеты, Страницы, Макросы* и *Модули.* Окно базы также содержит свою панель инструментов.

Следующий шаг – создание таблиц для хранения данных. К основным объектам Access помимо таблиц относятся запросы, отчеты, формы, макросы и модули. Но надо помнить, что таблица – основа базы данных, и все другие объекты зависят от данных таблиц.

Основные объекты базы данных Access можно создавать в режиме *Мастер* и в режиме *Конструктор*.

4.1. Таблицы

Таблицы – это основные объекты любой базы данных, в которых хранятся все данные, имеющиеся в базе, а также структура базы (поля, их типы и свойства). Все другие объекты (формы, отчеты, запросы) зависят от данных таблиц.

Создание таблиц с помощью мастера производится путем выбора типовой таблицы («Сотрудники», «Заказы» и т.д.) и необходимых полей из типовой таблицы или нескольких типовых таблиц. Выбранные имена полей можно редактировать. После ввода имени таблицы выбирается ключевое поле, позволяющее осуществлять связи между таблицами в базе данных.

При создании таблицы в режиме *Конструктор* выводится пустая структура таблицы, в которую необходимо ввести имена полей, указать типы данных в полях и задать размеры полей. В нижней части бланка структуры таблицы задаются свойства полей таблицы, позволяющие изменять способы хранения и отображения данных.

Поля таблиц базы данных не просто определяют структуру базы – они еще определяют групповые свойства данных, записываемых в ячейки, принадлежащие каждому из полей. Ниже перечислены основные свойства полей таблиц баз данных на примере СУБД Microsoft Access.

Характеристики полей базы данных:

- имя поля определяет, как следует обращаться к данным этого поля при автоматических операциях с базой (по умолчанию имена полей используются в качестве заголовков столбцов таблиц);
- тип поля определяет тип данных, которые могут содержаться в данном поле;
- размер поля определяет предельную длину (в символах) данных, которые могут размещаться в данном поле;
- формат поля определяет способ форматирования данных в ячейках, принадлежащих полю;
- маска ввода определяет форму, в которой вводятся данные в поле (средство автоматизации ввода данных);

- подпись определяет заголовок столбца таблицы для данного поля (если подпись не указана, то в качестве заголовка столбца используется свойство *Имя поля*);
- значение по умолчанию – то значение, которое вводится в ячейки поля автоматически (средство автоматизации ввода данных);
- условие на значение – ограничение, используемое для проверки правильности ввода данных (средство автоматизации ввода, которое используется, как правило, для данных, имеющих числовой тип, денежный тип или тип даты);
- сообщение об ошибке – текстовое сообщение, которое выдается автоматически при попытке ввода в поле ошибочных данных (проверка ошибочности выполняется автоматически, если задано свойство *Условие на значение*);
- обязательное поле – свойство, определяющее обязательность заполнения данного поля при наполнении базы;
- пустые строки – свойство, разрешающее ввод пустых строковых данных (от свойства *Обязательное поле* отличается тем, что относится не ко всем типам данных, а лишь к некоторым, например к текстовым);
- индексированное поле – если поле обладает этим свойством, то все операции, связанные с поиском или сортировкой записей по значению, хранящемуся в данном поле, существенно ускоряются. Кроме того, для индексированных полей можно сделать так, что значения в записях будут проверяться по этому полю на наличие повторов, что позволяет автоматически исключить дублирование данных.

Панель инструментов позволяет производить ряд операций с данными таблицы, такими, как сохранение, печать, сортировка, фильтрация, поиск. Перед печатью таблицы необходимо установить параметры страницы и сделать предварительный просмотр.

4.2. Запросы

Эти объекты служат для извлечения данных из таблиц и предоставления их пользователю в удобном виде. С помощью запросов выполняют такие операции, как отбор данных, их сортировку и фильтрацию, а также преобразование данных по заданному алгоритму, создание новых таблиц, автоматическое заполнение таблиц

данными, импортированными из других источников, выполнение вычислений и многое другое. Для разных действий создаются запросы разных типов.

Запрос-выборка предназначен для отбора данных, хранящихся в таблицах, и не изменяет эти данные.

Запрос-изменение используется для изменения или перемещения данных. К этому типу относятся: запрос на добавление записей, запрос на удаление записей, запрос на создание таблицы, запрос на обновление.

Запрос с параметром позволяет определить одно или несколько условий отбора во время выполнения запроса.

Ряд запросов строятся с использованием мастеров. Возможно создание запросов следующих видов:

- *простой запрос*, позволяющий выбирать поля из нескольких таблиц или запросов;
- *перекрестный запрос* вычисляет сумму, среднее значение, число элементов и значения других статистических функций, группируя данные и выводя их в компактном виде;
- *повторяющиеся записи* выполняют поиск одинаковых записей по какому-либо полю в таблице;
- *записи без подчиненных* находят все записи, не имеющие соответствующих записей в другой (связанной) таблице.

После выбора *Конструктора* при создании запроса Access предлагается использовать бланк запроса по примеру QBE.

Для формирования условий отбора полезным является использование *Построителя выражений*, который запускается из контекстного меню, связанного со строкой *Поле* или *Условие отбора* на бланке запроса QBE. Особенно удобно пользоваться *Построителем выражений* при конкатенации текста – объединении в форме или отчете текстовых значений из нескольких полей.

При составлении выражений используется несколько простых правил. Во-первых, выражение имеет всегда логический тип, т.е. его значение должно быть Да или Нет. В бланке запроса опускается часть выражения, содержащая имя поля, потому что оно задано в той же колонке. Во-вторых, существуют определенные требования к

синтаксису выражения: имена полей заключаются в квадратные скобки, а символьные контакты – в кавычки. Имя объекта базы данных (таблицы, формы или запроса) отделяется от имени поля восклицательным знаком.

Окно построителя имеет четыре области со своими полосами прокрутки. В верхней области располагается создаваемое выражение. Три нижние используются для выбора элементов. Они заполняются по иерархическому принципу. Левая область содержит список всех источников данных для запроса. Средний список служит для показа элементов, входящих в выбранный объект из левого списка. На рисунке в левом списке указаны имя запроса (Запрос 1) и имена таблиц и других объектов базы, а в средней части – имена полей, входящих в этот запрос или таблицу (*Фамилия, Имя*). Правый список служит для выбора объектов. Кнопки с символами математических операций позволяют быстро вводить соответствующие символы в выражение.

Кроме традиционных математических действий существует еще несколько специальных операторов.

BETWEEN AND заменяет знаки «больше или равно» и «меньше или равно». Например, условие BETWEEN 1981 AND 1984 эквивалентно условию > =1981 AND<=1984.

Знак «^» определяет возведение в степень.

Знак «&» используется для сложения данных символьного типа. Для соединения можно использовать и более привычный знак «+». Например, эквивалентны следующие три выражения: «Петров», «Петр» & «ов», «Петр» + «ов».

Оператор LIKE используется для создания масок при определении строк с неизвестными символами и требует дополнительных специальных символов:

? – обозначает любой одиночный символ;

- обозначает любую последовательность символов;

- обозначает любую цифру;

[ ] – обозначает символ из определенного набора в квадратных скобках, например [a - d] обозначает одну из четырех букв: a, b, d. Восклицательный знак инвертирует смысл выражения, заключенного в квадратные скобки: [!1 - 5] – исключает цифры от 1 до 5.

Также для построения условий отбора могут использоваться логические операторы: AND, EQV, OR.

4.3. Формы

Формы – это средства для ввода данных. Назначение форм – представлять пользователю средства для заполнения только тех полей, которые ему нужно заполнять. Одновременно с этим в форме можно разместить специальные элементы управления (счетчики, раскрывающиеся списки, переключатели, флажки и т. п.) для автоматизации ввода.

Преимущества форм раскрываются особенно наглядно, когда происходит ввод данных с заполненных бланков. В этом случае форму делают графическими средствами так, чтобы она повторяла оформление бланка, - это заметно упрощает работу наборщика, снижает его утомляемость и предотвращает появление печатных ошибок. Формы могут содержать графики и диаграммы и иметь специальные поля с функциями. В Access существует несколько режимов создания формы: *Автоформа, Мастер форм, Конструктор форм.*

Самый простой способ создания формы – *Автоформа.*

Форма позволяет вводить, просматривать, редактировать и печатать данные.

4.4. Отчеты

По своим свойствам и структуре отчеты во многом похожи на формы, но предназначены только для вывода данных, причем для вывода не на экран, а на печатающее устройство (принтер). В связи с этим отчеты отличаются тем, что в них приняты специальные меры для группировки выводимых данных и для вывода специальных элементов оформления, характерных для печатных документов (верхний и нижний колонтитулы, номера страниц, служебная информация о времени создания отчета). Отчеты могут содержать данные из нескольких таблиц или запросов.

Можно создать отчеты следующих видов:

- простая распечатка из режима Таблицы или Формы, используемая как черновой вариант отчета;

- детальный отчет – хорошо подготовленный отчет в наглядном удобном виде, включающий ряд дополнительных элементов;
- специальный отчет, позволяющий подготавливать, к примеру, почтовые наклейки и формы писем.

4.5. Макросы и модули

Эти категории объектов предназначены как для автоматизации повторяющихся операций при работе с СУБД, так и для создания новых функций путем программирования. В СУБД Access макросы состоят из последовательности внутренних команд СУБД и являются одним из средств автоматизации работы с базой.

Модули создаются средствами внешнего языка программирования, в данном случае языка Visual Basic for Applications. Это одно из средств, с помощью которых разработчик базы может заложить функциональные нестандартные возможности, удовлетворить специфические требования заказчика, повысить быстродействие системы управления, а также уровень ее защищенности.

4.6. Связь между таблицами и целостность данных

Рассмотрим, как реализуется установка связей между таблицами на практике.

Между одноименными полями двух таблиц MS Access автоматически устанавливает связь. Например, между таблицами «Студенты» и «Успеваемость» устанавливается связь по полю «№ студ. билета». Это означает, что при формировании запроса к этой паре таблиц Access сможет объединить записи (строки) таблиц, в которых значения поля «№ студ. билета» совпадают.

Кроме того, Access позволяет вручную установить связь между таблицами по разноименным полям, однако этой возможностью лучше не пользоваться, так как это запутывает и аналитиков, и пользователей.

В общем случае допускается связь по двум, трем и более одноименным полям, но для простоты изложения мы этот случай не рассматриваем.

Итак, если установлена связь между двумя таблицами (автоматически или вручную), данные из обеих таблиц можно объединить. Иногда этого достаточно,

однако при создании серьезных баз данных нам придется позаботиться о дополнительных средствах контроля связанных данных, вводимых в разные таблицы. Например, при ведении таблицы «Успеваемость» нельзя допустить случайный ввод в эту таблицу данных о несуществующих студентах, нельзя удалять из таблицы «Студенты» записи о студентах, о которых хранятся данные об успеваемости.

Механизм, который обеспечивает согласованность данных между двумя связанными таблицами, называется поддержкой целостности данных. Чтобы обеспечить целостность данных, при установлении связи между двумя таблицами нужно активизировать переключатель. Если пользователь включил механизм поддержки целостности, то он должен одновременно указать тип связи: «один к одному» или «один ко многим».

Целостность данных означает следующее:

- в связанное поле подчиненной таблицы можно вводить только те значения, которые имеются в связанном поле главной таблицы (например, в таблицу «Успеваемость» нельзя ввести запись с номером студенческого билета, отсутствующим в таблице «Студенты»);
- из главной таблицы нельзя удалить запись, у которой значение связанного поля совпадает хотя бы с одним значением того же поля в подчиненной таблице (например, из таблицы «Студенты» нельзя удалить «№ студ. Билета», который еще не удален из таблицы «Успеваемость»).

При попытке нарушить эти запреты MS Access выдает сообщение об ошибке.

Включив механизм поддержки целостности, вы можете (но не обязаны) указать, чтобы при модификации данных система запускала следующие процессы:

- каскадное обновление связанных полей;
- каскадное обновление связанных записей.

Каскадное обновление означает, что изменение связанного поля в главной таблице (например, код клиента) автоматически будет и в связанных записях подчиненной таблицы.

Установление связей между таблицами рассмотрим на конкретном примере – на нашей базе данных «Колледж».

Выберите команду *Правка /Схема данных*. На экране появится диалоговое окно со списком всех таблиц открытой базы данных.

Можно включить в этот список и запросы (или создать список только из запросов).

Задача пользователя – указать системе те таблицы, между которыми он устанавливает связи. Нужно выделить таблицу «Преподаватели» и нажать кнопку *Добавить*, затем то же самое проделать с таблицами «Успеваемость» и «Студенты». Нажать кнопку *Закрыть*.

На экране появится окно *Схема данных*.

Это окно содержит все таблицы базы данных, между которыми устанавливаются (или уже установлены) связи. Для установления связи между двумя таблицами можно методом «Drag-and-Drop» переместить имя поля с первичным ключом главной таблицы на одноименное поле подчиненной таблицы.

Прежде всего, нужно установить связь между таблицами «Студенты» и «Успеваемость». Удерживая нажатой левую кнопку мыши, переместите № студ. билета из таблицы «Студенты» на № студ. билета в таблице «Успеваемость» и отпустите левую кнопку мыши. На экране появится диалоговое окно Связи. В этом окне установите флажок «Обеспечение целостности данных». Этим вы включите механизм поддержки целостности данных в таблицах «Студенты» и «Успеваемость».

После активизации флажка «Обеспечение целостности данных» становятся допустимыми радиокнопки Отношение и два флажка каскадных операций. В группе «Отношение» надо обязательно выбрать один из типов связи: «один-к-одному» или «один-ко-многим».

Кроме того, вы можете (если хотите) установить любой флажок (или оба) каскадной модификации – обновления или удаления. Нажмите кнопку Создать. На экране вновь появится окно Схема данных с графическим изображением установленной связи.

4.7. Сервисные операции

1) **Проверка орфографии. О**беспечивают авто-исправление ошибок ввода. Используется словарь. Включается система и при обнаружении слова, отсутствующего в словаре, появляется диалоговое окно "Орфография". Можно это слово пропустить, добавить в словарь, заменить.
2) **Автозамена**. Автоматически исправляет ошибки и опечатки непосредственно в процессе набора данных в базу. Список автозамены "общий" для MS Office 2003. Есть много настроек как делать замену.
3) **Устранение конфликтов в ЛВС.** На удаленных рабочих станциях пользователи могут работать с копиями БД, а затем делать их синхронизацию (запуск - Меню\Сервис**Репликация**\Устранить конфликты).
4) **Средства анализа БД.** Позволяют оптимизировать построение БД, документировать ее состояние, исключить повторы данных в таблицах, повысить производительность.
5) **Средства защиты БД.** Позволяют предотвратить умышленные или случайные операции (просмотр, изменение, удаление информации) лицами, которые не имеют соответствующих прав доступа (это особенно важно в ЛВС). **Способы защиты** – это установить пароль на открытие БД, ввести рабочую группу, ограничение доступа, изменение прав владения, шифрование БД.
6) **Репликация** предоставляет пользователям, которые работают за различными компьютерами, удобный способ обмена изменениями, вносимыми в единую БД. Репликация имеет широкое практическое применение. Для создания и синхронизации реплик в MS Access 2003 предусмотрены команды репликации.

5. Тестовые задания для самопроверки

1. Основным элементом табличной (реляционной) базы данных является …
2. Структура базы данных в Access изменится, если …
3. Графический образ базы данных в Access, задающий ее структуру и связи, обеспечивающий целостность данных для взаимосвязанных таблиц, называется …

4. Тип данных, обеспечивающий запись в одном поле таблицы Access до 64000 символов, называется …
5. Модель базы данных, представляющая собой совокупность двумерных таблиц, в которой каждая таблица отражает тип объекта реального мира, а каждая строка в таблице отражает параметры конкретного элемента объекта, называется …
6. Интерфейс, упрощающий работу пользователя с готовой базой данных, создаваемый автоматически в Access, называется …
7. Выбрать необходимые данные из одной или нескольких взаимосвязанных таблиц в Access, отобрать нужные поля, произвести вычисления и получить результат в виде новой таблицы, можно с помощью …
8. База данных, объекты и настроечные параметры Access всегда находятся в файлах с расширением …
9. Для представления данных из таблиц Access в формате Word их необходимо сохранить в файлах с расширением …
10. Практически вся защита для базы данных в Access теряется, если к этой базе применить операцию …
11. Язык запросов и программирования баз данных - это …
12. .mdb – это расширение в имени файлов, создаваемых программой ...

Вопросы для самопроверки к лекции № 7

1. Что такое база данных?
2. Что такое компьютерные базы данных?
3. Каково назначение баз данных?
4. Каковы единицы измерения информации?
5. Какова классификация компьютерных сетей?
6. Цифровые базы данных?
7. Текстовые базы данных?

ЛЕКЦИЯ № 8

Раздел 3. Основы информационной и компьютерной безопасности

Урок № 28

Количество часов: 2

Цель: Изучение проблем компьютерной безопасности и организации защиты информации от компьютерных вирусов.

План лекции:

1. Безопасность в информационной среде.
    1.1. Компьютерная преступность.
    1.2. Предупреждение компьютерных преступлений.
    1.3. Защита данных.
2. Компьютерные вирусы и антивирусные программы.
    2.1. Классификация вирусов.
    2.2. Методы защиты от компьютерных вирусов**.**

1. Безопасность в информационной среде

Изменения, происходящие в экономической жизни России - создание финансово-кредитной системы, предприятий различных форм собственности и т.п. - оказывают существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность - государственная, поэтому информация и секреты были тоже только государственные, которые охранялись мощными спецслужбами.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

В этом смысле компьютер может выступать и как предмет посягательств, и как инструмент. Если разделять два последних понятия, то термин компьютерное преступление как юридическая категория не имеет особого смысла. Если компьютер - только объект посягательства, то квалификация правонарушения может быть

произведена по существующим нормам права. Если же - только инструмент, то достаточен только такой признак, как “применение технических средств”. Возможно объединение указанных понятий, когда компьютер одновременно и инструмент и предмет. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Также если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами РФ.

Каждый сбой работы компьютерной сети это не только “моральный” ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, “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 в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать: целостность данных - защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных. Конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

1.1. Компьютерная преступность

Ни в одном из уголовных кодексов союзных республик не удастся найти главу под названием “Компьютерные преступления”. Таким образом, компьютерных

преступлений, как преступлений специфических в юридическом смысле не существует.

Попытаемся кратко обрисовать явление, которое как социологическая категория получила название “компьютерная преступность”. Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров.

1. Несанкционированный доступ к информации, хранящейся в компьютере. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры “электронные корсары”, “компьютерные пираты” - так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая на удачу один номер за другим, они терпеливо дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем часто банальны), то можно внедриться в чужую компьютерную систему.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, как покупатель рассматривает товары на витрине.

2. Ввод в программное обеспечение “логических бомб”, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

“Временная бомба” - разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени.

Способ “троянский конь” состоит в тайном введении в чужую программу таких команд, позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

С помощью “троянского коня” преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

В США получила распространение форма компьютерного вандализма, при которой “троянский конь” разрушает через какой-то промежуток времени все программы, хранящиеся в памяти машины. Во многих поступивших в продажу компьютерах оказалась “временная бомба”, которая “взрывается” в самый неожиданный момент, разрушая всю библиотеку данных. Не следует думать, что “логические бомбы” - это экзотика, несвойственная нашему обществу.

3. Разработка и распространение компьютерных вирусов.

“Троянские кони” типа “сотри все данные этой программы, перейди в следующую и сделай тоже самое” обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Выявляется вирус не сразу: первое время компьютер “вынашивает инфекцию”, поскольку для маскировки вирус не нередко используется в комбинации с “логической бомбой” или “временной бомбой”. Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Все происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека.

Начиная действовать (перехватывать управление), вирус дает команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает программе управление. Пользователь ничего не заметит, так как его компьютер находится в состоянии “здорового носителя вируса”. Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер “заболевает”.

4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т.п.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти не достижима.

5. Подделка компьютерной информации.

По-видимому, этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию. Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели.

6. Хищение компьютерной информации.

Если “обычные” хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше,

машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

Собственность на информацию, как и прежде, не закреплена в законодательном порядке. На мой взгляд, последствия этого не замедлят сказаться.

1.2. Предупреждение компьютерных преступлений

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на предупреждение преступления. Выделим из них технические, организационные и правовые.

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам отнесем охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

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 за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашение

1.3. Защита данных

Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономном). Остановимся подробнее на первом типе, представляющем большой интерес. Наиболее распространены два алгоритма.

Стандарт шифрования данных DES (Data Encryption Standart) был разработан фирмой IBM в начале 70-х годов и в настоящее время является правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией Американских Банкиров. Сложный алгоритм DES использует ключ длиной 56 бит и 8 битов проверки на четность и требует от злоумышленника перебора 72 квадрилионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм удовлетворительно решает проблему превращения конфиденциальной информации в недоступную.

Защита от компьютерных вирусов. В качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера. Корпорация Intel в 1994 году предложила перспективную технологию защиты от вирусов в компьютерных сетях. Flash-память сетевых адаптеров Intel EtherExpress PRO/10 содержит антивирусную программу, сканирующую все системы компьютера еще до его загрузки.

Защита от несанкционированного доступа. Помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых операционных систем. Так, крупнейший производитель сетевых ОС - корпорация

Novell - в своем последнем продукте NetWare 4.1 предусмотрел помимо стандартных средств ограничения доступа, таких, как система паролей и разграничения полномочий, ряд новых возможностей, обеспечивающих первый класс защиты данных. Новая версия NetWare предусматривает, в частности, возможность кодирования данных по принципу “открытого ключа” (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов.

В то же время в такой системе организации защиты все равно остается слабое место: уровень доступа и возможность входа в систему определяются паролем. Не секрет, что пароль можно подсмотреть или подобрать. Для исключения возможности неавторизованного входа в компьютерную сеть в последнее время используется комбинированный подход - пароль + идентификация пользователя по персональному “ключу”. В качестве “ключа” может использоваться пластиковая карта (магнитная или со встроенной микросхемой - smart-card) или различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза или отпечатков пальцев, размерам кисти руки и так далее.

Защита информации при удаленном доступе. По мере расширения деятельности предприятий, роста численности персонала и появления новых филиалов, возникает необходимость доступа удаленных пользователей (или групп пользователей) к вычислительным и информационным ресурсам главного офиса компании. Разработаны специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям. Например, фирмой AT&T предлагается модуль Remote Port Security Device (PRSD), представляющий собой два блока размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют установить несколько уровней защиты и контроля доступа.

Широкое распространение радиосетей в последние годы поставило разработчиков радиосистем перед необходимостью защиты информации от “хакеров”, вооруженных разнообразными сканирующими устройствами. Были применены разнообразные технические решения. Например, в радиосети компании RAM Mobil Data информационные пакеты передаются через разные каналы и базовые станции, что делает практически невозможным для посторонних собрать всю

передаваемую информацию воедино. Активно используются в радио сетях и технологии шифрования данных при помощи алгоритмов DES и RSA.

Никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях.

В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.

2. Компьютерные вирусы и антивирусные программы

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам, а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется «зараженной». Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и «заражает» другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, «засоряет» оперативную память и т.д.). Вирус - это программа, обладающая способностью к самовоспроизведению. Такая способность является единственным свойством, присущим всем типам вирусов.

История компьютерной вирусологии представляется сегодня постоянной «гонкой за лидером», причем, не смотря на всю мощь современных антивирусных программ, лидерами являются именно вирусы. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, использующими действительно принципиально новые идеи. Все остальные – «вариации на тему». Но каждая оригинальная разработка заставляет создателей антивирусов приспосабливаться к новым условиям, догонять вирусную технологию. Последнее можно оспорить. Например, в 1989 году американский студент сумел создать вирус, который вывел из строя около 6000 компьютеров Министерства обороны США. Или эпидемия известного вируса Dir-II, разразившаяся в 1991 году. Вирус использовал действительно оригинальную, принципиально новую технологию и на первых порах

сумел широко распространиться за счет несовершенства традиционных антивирусных средств.

Или всплеск компьютерных вирусов в Великобритании: Кристоферу Пайну удалось создать вирусы Pathogen и Queeq, а также вирус Smeg. Именно последний был самым опасным, его можно было накладывать на первые два вируса, и из-за этого после каждого прогона программы они меняли конфигурацию. Поэтому их было невозможно уничтожить. Чтобы распространить вирусы, Пайн скопировал компьютерные игры и программы, заразил их, а затем отправил обратно в сеть. Пользователи загружали в свои компьютеры зараженные программы и инфицировали диски. Ситуация усугубилась тем, что Пайн умудрился занести вирусы и в программу, которая с ними борется. Запустив ее, пользователи вместо уничтожения вирусов получали еще один. В результате этого были уничтожены файлы множества фирм, убытки составили миллионы фунтов стерлингов.

Причины появления и распространения компьютерных вирусов, с одной стороны, скрываются в психологии человеческой личности и ее теневых сторонах (зависти, мести, тщеславии непризнанных творцов, невозможности конструктивно применить свои способности), с другой стороны, обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы персонального компьютера.

2.1. Классификация вирусов

В зависимости от среды обитания вирусы можно разделить на:

Сетевые вирусы распространяются по различным компьютерным сетям.

Файловые вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord).

Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на:

Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего дискеты.

Что происходит, когда вы включаете компьютер? Первым делом управление передается программе начальной загрузки, которая хранится в постоянно запоминающем устройстве (ПЗУ) т.е. ПНЗ ПЗУ.

Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе А:

Таким образом, нормальная схема начальной загрузки следующая:

ПНЗ (ПЗУ) - ПНЗ (диск) – СИСТЕМА.

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части: голову и т. н. хвост. Хвост может быть пустым.

Пусть у вас имеются чистая дискета и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва - в нашем случае не защищенная от записи и еще не зараженная дискета, он приступает к заражению. Заражая дискету, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad);
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой;

– организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке ПНЗ (ПЗУ) - ПНЗ (диск) – СИСТЕМА появляется новое звено: ПНЗ (ПЗУ) - ВИРУС - ПНЗ (диск) - СИСТЕМА

Мы рассмотрели схему функционирования простого бутового вируса, живущего в загрузочных секторах дискет. Как правило, вирусы способны заражать не только загрузочные секторы дискет, но и загрузочные секторы винчестеров.

Файловые вирусы. В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрим схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл. При запуске такого файла вирус получает управление, производит некоторые действия и передает управление "хозяину"

Какие же действия выполняет вирус? Он ищет новый объект для заражения - подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции - размножения, вирус вполне может сделать что-нибудь замысловатое (сказать, спросить, сыграть) - это уже зависит от фантазии автора вируса. Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код - следовательно, заражение исполняемого файла всегда можно обнаружить.

Полиморфные вирусы. Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку "по ходу дела", может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Стелс-вирусы. В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода/вывода BIOS. Ряд вирусов, после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он на ходу подменяет читаемые данные, как, будто вируса на диске нет.

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-механизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске, и легко обнаружит вирус.

2.2. Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации (копирование важной информации и разграничение доступа);
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов:

ПРОГРАММЫ-ДЕТЕКТОРЫ позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение (Scan, Aidstest).

Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".

Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, а они перехватываются вирусом, который говорит, что все хорошо.

Так что надежный диагноз программы-детекторы дают только при загрузке DOS с «чистой», защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с этой дискеты.

Большинство программ-детекторов имеют функцию «доктора», т.е. они пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.

Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают.

ПРОГРАММЫ-РЕВИЗОРЫ имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Чтобы проверка состояния программ и дисков проходила при каждой загрузке операционной системы, необходимо включить команду запуска программы-ревизора в командный файл AUTOEXEC. BAT. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда. Более того, та же программа-ревизор сможет найти поврежденные вирусом файлы.

ПРОГРАММЫ-ФИЛЬТРЫ, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не «ловят» подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны - они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

ПРОГРАММЫ-ВАКЦИНЫ, или ИММУНИЗАТОРЫ, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Вопросы для самопроверки к лекции № 8

1. Назовите меры защиты компьютерной информации.

2. Какие средства программно-аппаратного уровня защиты вы знаете?
3. Как защититься от вирусной атаки?