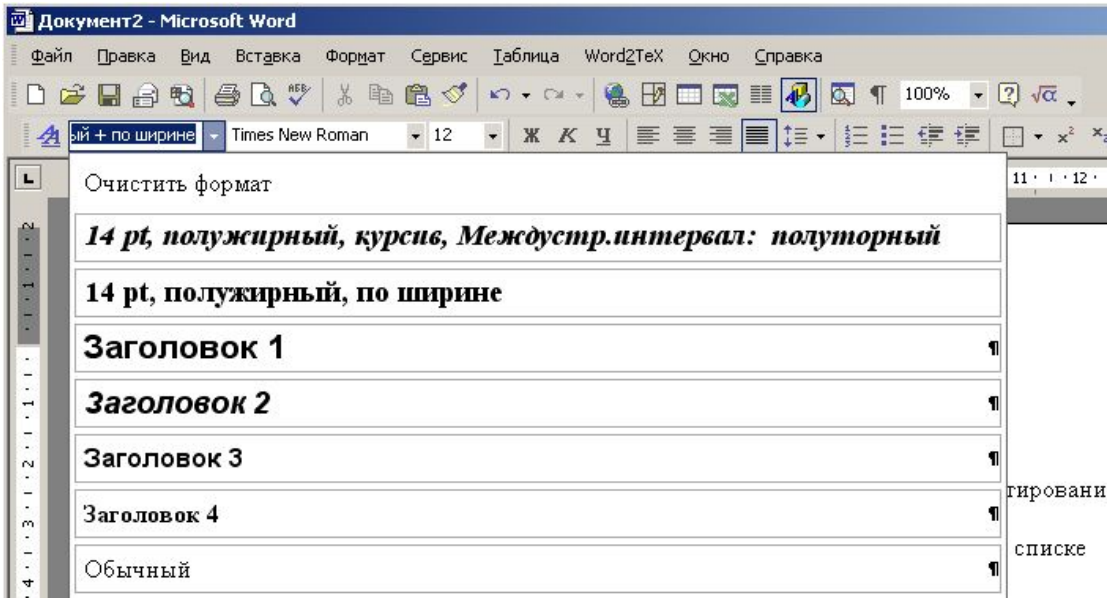
Лекция

Текстовый редактор WORD

Часть 5. Стили. Оглавления.
Перекрестные ссылки. Гиперссылки

Стиль

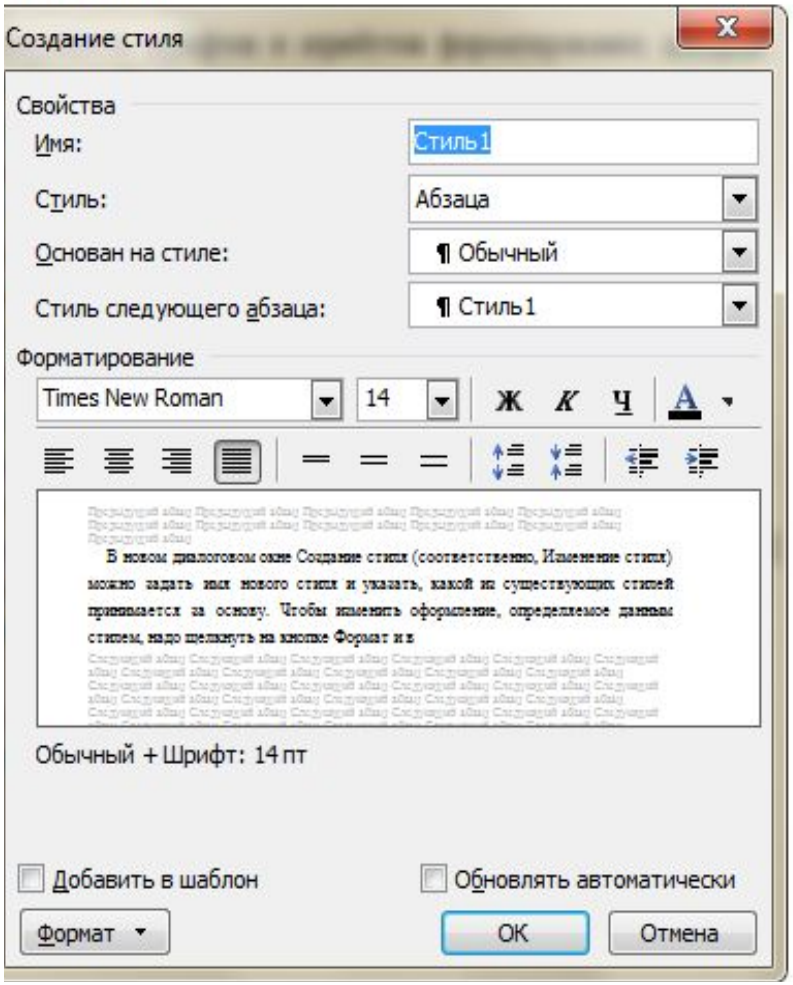
Стиль – это совокупность шрифтов и атрибутов форматирования, которой присвоено некоторое имя.
Доступные стили перечислены в раскрывающемся списке "Стиль" на панели инструментов "Форматирование"



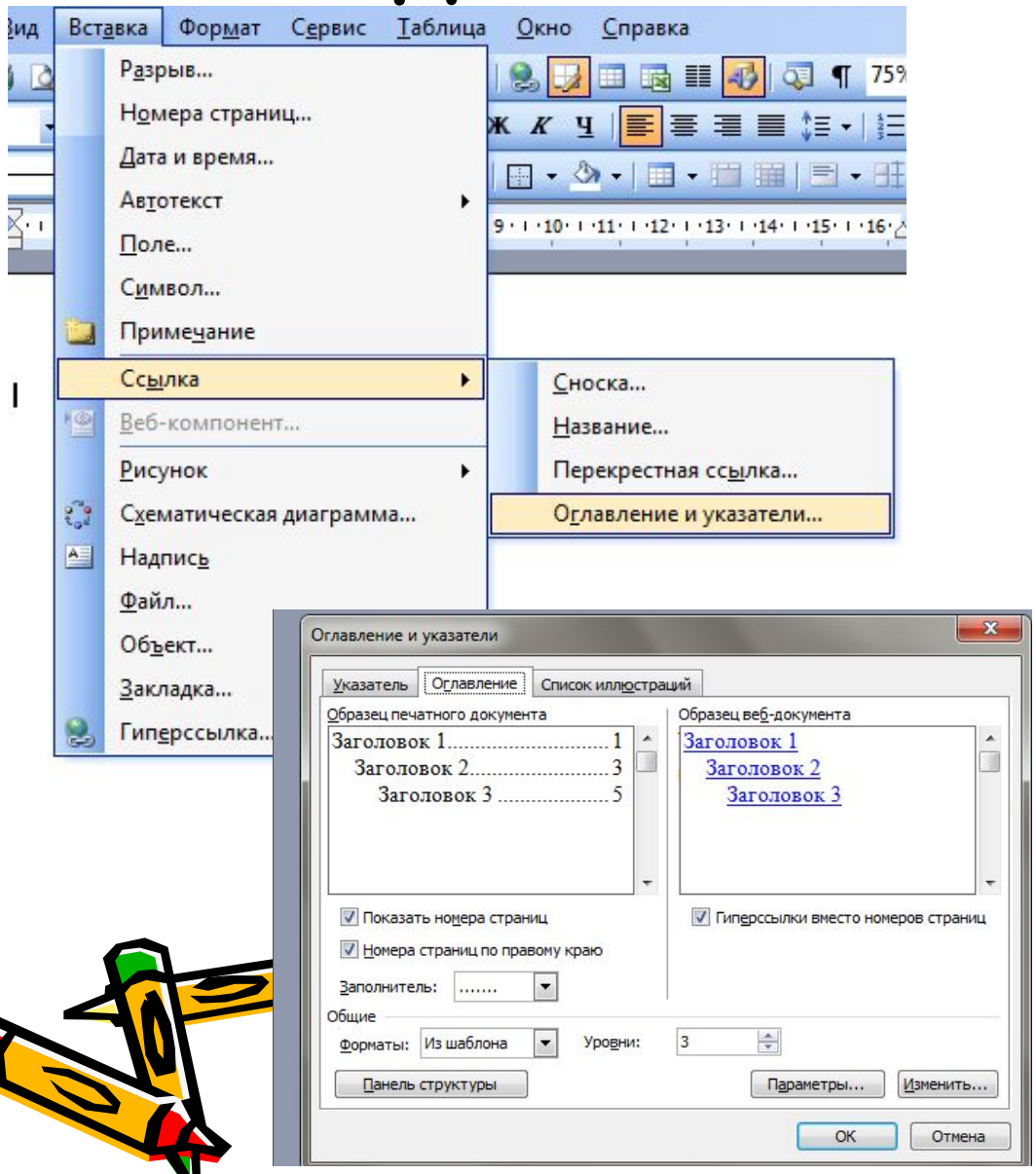
Создание стиля

Для создания нового стиля следует выполнить команду **Формат > Стиль.**

В диалоговом окне **Стиль** можно щелкнуть на кнопке **Создать** (для создания нового стиля) или **Изменить** (для изменения существующего стиля).

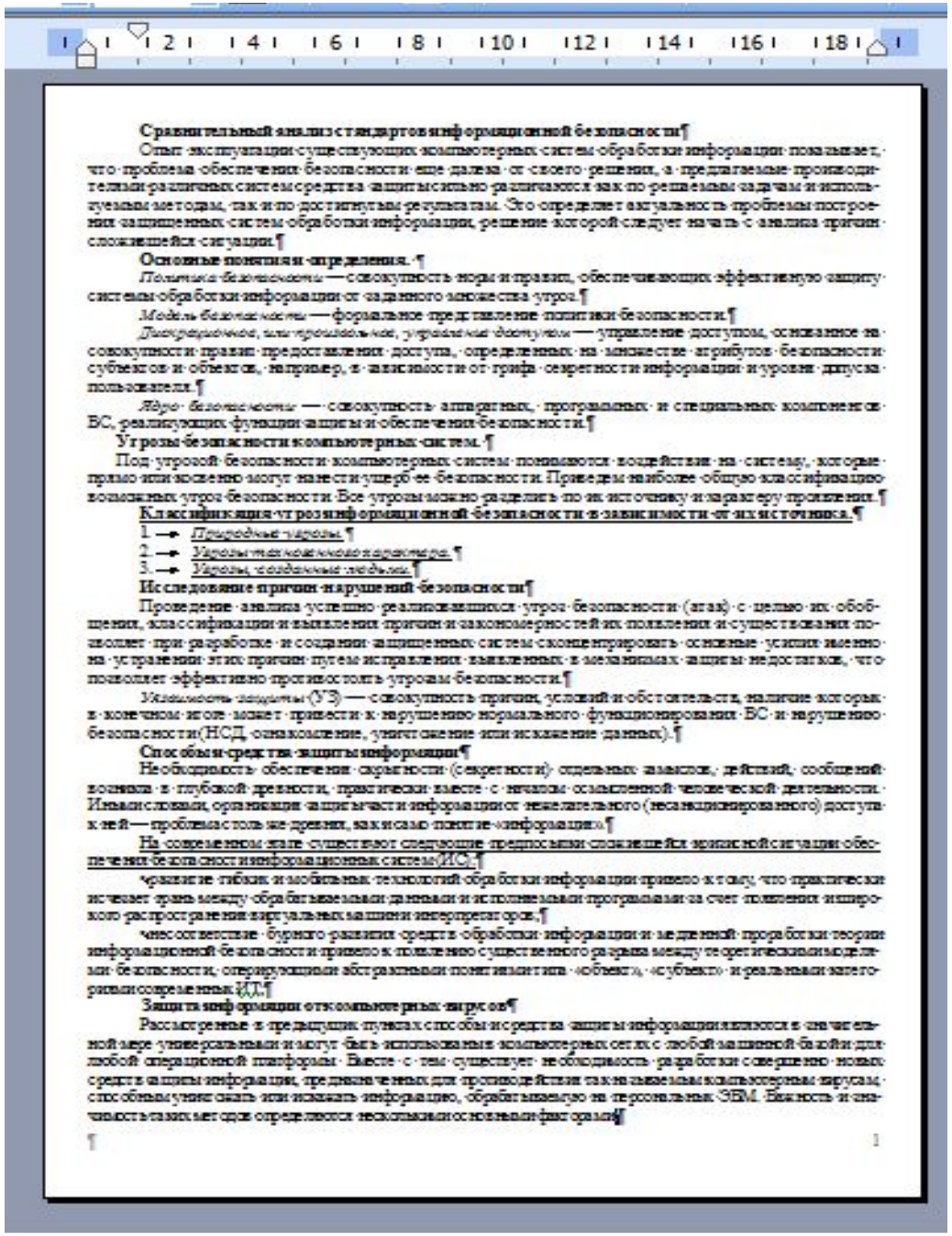


Создание оглавления



- Оформить стилями заголовков все заголовки, которые должны быть занесены в оглавление;
- Поместить курсор в то место документа, куда должно быть вставлено оглавление;
- Выполнить команду **Вставка - Оглавление и указатели**... и выбрать вкладку **Оглавление (или Вставка-Ссылка-Оглавление и указатели)**;
- Нажать **ОК**.

Исходный текст



Сравнительный анализ стандартов информационной безопасности

Опыт эксплуатации существующих компьютерных систем обработки информации показывает, что проблема обеспечения безопасности еще далека от своего решения, а предлагаемые производителями различных систем средства защиты сильно различаются как по решаемым задачам и используемым методам, так и по достигнутым результатам. Это определяет актуальность проблемы построения защищенных систем обработки информации, решение которой следует начать с анализа причин сложившейся ситуации.

Основные понятия и определения.

Политика безопасности — совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз.

Модель безопасности — формальное представление политики безопасности.

Дискреционное, или произвольное, управление доступом — управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от грифа секретности информации и уровня допуска пользователя.

Ядро безопасности — совокупность аппаратных, программных и специальных компонентов ВС, реализующих функции защиты и обеспечения безопасности.

Угрозы безопасности компьютерных систем.

Под угрозой безопасности компьютерных систем понимаются воздействия на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Приведем наиболее общую классификацию возможных угроз безопасности. Все угрозы можно разделить по их источнику и характеру проявления.

Классификация угроз информационной безопасности в зависимости от их источника.

1. *Природные угрозы.*
2. *Угрозы техногенного характера.*
3. *Угрозы, создаваемые людьми.*

Исследование причин нарушений безопасности

Проведение анализа успешно реализовавшихся угроз безопасности (атак) с целью их обобщения, классификации и выявления причин и закономерностей их появления и существования позволяет при разработке и создании защищенных систем сконцентрировать основные усилия именно на устранении этих причин путем исправления выявленных в механизмах защиты недостатков, что позволяет эффективно противостоять угрозам безопасности.

Уязвимость защиты (УЗ) — совокупность причин, условий и обстоятельств, наличие которых в конечном итоге может привести к нарушению нормального функционирования ВС и нарушению безопасности (НСД, ознакомление, уничтожение или искажение данных).

Способы и средства защиты информации

Необходимость обеспечения скрытности (секретности) отдельных замыслов, действий, сообщений возникла в глубокой древности, практически вместе с началом осмысленной человеческой деятельности. Иными словами, организация защиты части информации от нежелательного (несанкционированного) доступа к ней — проблема столь же древняя, как и само понятие «информация».

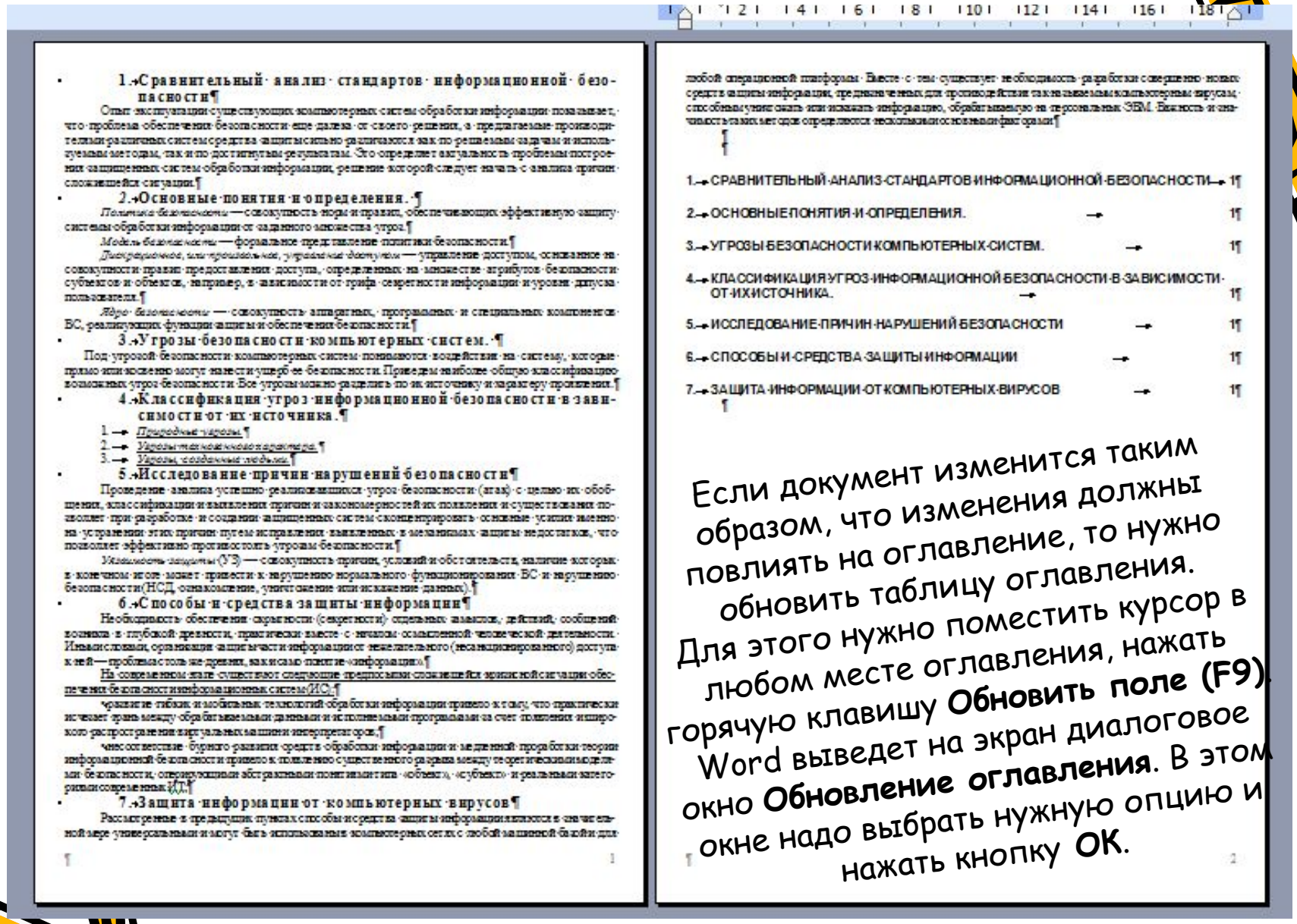
На современном этапе существуют следующие предпосылки сложившейся кризисной ситуации обеспечения безопасности информационных систем (ИС).

Появление гибких и мобильных технологий обработки информации привело к тому, что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счет появления и широкого распространения виртуальных машин интерпретаторов.

Несоответствие бурного развития средств обработки информации и медленной проработки теории информационной безопасности привело к появлению существенного разрыва между теоретическими моделями безопасности, оперирующими абстрактными понятиями типа «объект», «субъект» и реальными категориями современных ИТ.

Защита информации от компьютерных вирусов

Рассмотренные в предыдущих пунктах способы и средства защиты информации являются в значительной мере универсальными и могут быть использованы компьютерных сетях с любой машинной базой для любой операционной платформы. Вместе с тем существует необходимость разработки совершенно новых средств защиты информации, предназначенных для противодействия так называемым компьютерным вирусам, способным уничтожать или искажать информацию, обрабатываемую на персональных ЭВМ. Важность и значимость таких методов определяются несколькими основными факторами.



1. Сравнительный анализ стандартов информационной безопасности

Опыт эксплуатации существующих компьютерных систем обработки информации показывает, что проблема обеспечения безопасности еще далека от своего решения, а предлагаемые производителями различных систем средства защиты сильно различаются как по решаемым задачам и используемым методам, так и по достигнутым результатам. Это определяет актуальность проблемы построения защищенных систем обработки информации, решение которой следует начать с анализа причин сложившейся ситуации.

2. Основные понятия и определения.

Политика безопасности — совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз.

Модель безопасности — формальное представление политики безопасности.

Дискреционное, или произвольное, управление доступом — управление доступом, основанное на совокупности правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от грифа секретности информации и уровня допуска пользователя.

Ядро безопасности — совокупность аппаратных, программных и специальных компонентов ВС, реализующих функции защиты и обеспечения безопасности.

3. Угрозы безопасности компьютерных систем.

Под угрозой безопасности компьютерных систем понимаются воздействия на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Приведем наиболее общую классификацию возможных угроз безопасности. Все угрозы можно разделить по их источнику и характеру проявления.

4. Классификация угроз информационной безопасности в зависимости от их источника.

1. *Природные угрозы*
2. *Угрозы техногенного характера*
3. *Угрозы, созданные людьми*

5. Исследование причин нарушений безопасности

Проведение анализа успешно реализовавшихся угроз безопасности (атак) с целью их обобщения, классификации и выявления причин и закономерностей их появления и существования позволяет при разработке и создании защищенных систем сконцентрировать основные усилия именно на устранении этих причин путем исправления выявленных в механизмах защиты недостатков, что позволит эффективно противостоять угрозам безопасности.

Уязвимость защиты (УЗ) — совокупность причин, условий и обстоятельств, наличие которых в конечном итоге может привести к нарушению нормального функционирования ВС и нарушению безопасности (НСД, ознакомление, уничтожение или искажение данных).

6. Способы и средства защиты информации

Необходимость обеспечения скрытности (секретности) отдельных замыслов, действий, сообщений возникла в глубокой древности, практически вместе с началом осознанной человеческой деятельности. Иными словами, организация защиты части информации от нежелательного (несанкционированного) доступа к ней — проблема столь же древняя, как и само понятие «информация».

На современном этапе существуют следующие предпосылки сложившейся кризисной ситуации обеспечения безопасности информационных систем (ИС):

- наличие гибких и мобильных технологий обработки информации прямого доступа, что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счет появления и широкого распространения виртуальных машин и интерпретаторов;
- несоответствие бурного развития средств обработки информации и медленной проработки теории информационной безопасности привело к появлению существенного разрыва между теоретическими моделями безопасности, оперирующими абстрактными понятиями типа «объект», «субъект» и реальными категориями современных ИТ.

7. Защита информации от компьютерных вирусов

Рассмотренные в предыдущих пунктах способы и средства защиты информации являются в значительной мере универсальными и могут быть использованы в компьютерных сетях с любой машинной базой и для любой операционной платформы. Вместе с тем существует необходимость разработки совершенно новых средств защиты информации, предназначенных для противодействия так называемым компьютерным вирусам, способным уничтожать или искажать информацию, обрабатываемую на персональных ЭВМ. Важность и значимость таких методов определяется несколькими основными факторами.

Если документ изменится таким образом, что изменения должны повлиять на оглавление, то нужно обновить таблицу оглавления. Для этого нужно поместить курсор в любом месте оглавления, нажать горячую клавишу **Обновить поле (F9)**. Word выведет на экран диалоговое окно **Обновление оглавления**. В этом окне надо выбрать нужную опцию и нажать кнопку **ОК**.

Перекрестные ссылки

Перекрестные ссылки могут быть текстовыми, ссылками на номера страниц или ссылками на номера соответствующего элемента.

Чтобы вставить перекрестную ссылку необходимо:

1. Выполнить команду **Вставка - Перекрестная ссылка (или Вставка-Ссылка-Перекрестная ссылка)**. На экране появится диалоговое окно **Перекрестная ссылка**.
2. Из списка **Тип ссылки** надо выбрать тип объекта, перекрестную ссылку на который вы хотите вставить. Для разных типов перекрестных ссылок набор опций в списке **Вставить ссылку на**… будет различным.
3. Выбрать из списка **Вставить ссылку на**… тот тип элемента, на который создается ссылка.
4. После этого название списка **Для какого**…. изменится и будет включать в себя выбранный тип ссылки. В этом списке будут видны все объекты выбранного типа, найденные в документе.
5. Выбрать объект, ссылка на который создается, из списка **Для какого**….
6. Щелкнуть кнопку **Вставить**.

Для вставки гиперссылки на существующий или новый документ, файл или веб-страницу необходимо выполнить следующие действия:

- Выделите текст или графический объект, который предполагается использовать как гиперссылку, а затем нажмите кнопку **Добавление гиперссылки** на панели управления **Стандартная**. (или **Вставка-Гиперссылка**)
- Выполните одно из следующих действий.

Создание связи с существующим файлом или веб-страницей

- В области **Связать с…** нажмите кнопку **файлом, веб- страницей**.
- Выполните одно из следующих действий.
  - Если известен адрес или файл, ссылку на который необходимо создать, можно сразу ввести его в поле **Адрес**.
  - Выберите одну из папок в списке **Папка**, а затем найдите и выделите нужный файл.

Создание связи с новым файлом

- В области **Связать с…** нажмите кнопку **Создать документ (**или **Новым документом)**.
- Введите имя нового файла. Можно также указать путь к новому файлу, а затем либо сразу открыть этот файл для правки, либо сделать это позже.
- При установке указателя на гиперссылку на экране появляется подсказка. Чтобы назначить подсказку для гиперссылки, нажмите кнопку **Подсказка**, а затем введите текст подсказки. Если текст подсказки не задан, вместо него отображается путь к файлу.