Тема 3: Система формирования режима информационной безопасности

Задачи информационной безопасности общества

- Анализ основ информационной безопасности показал, что обеспечение безопасности является задачей комплексной. С одной стороны режима информационной, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле "пронизаны" все сферы общественной деятельности и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

- В этой связи вполне закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

- Рассматривая проблему информационной безопасности в широком смысле, можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача по минимизации всех отрицательных последствий от всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

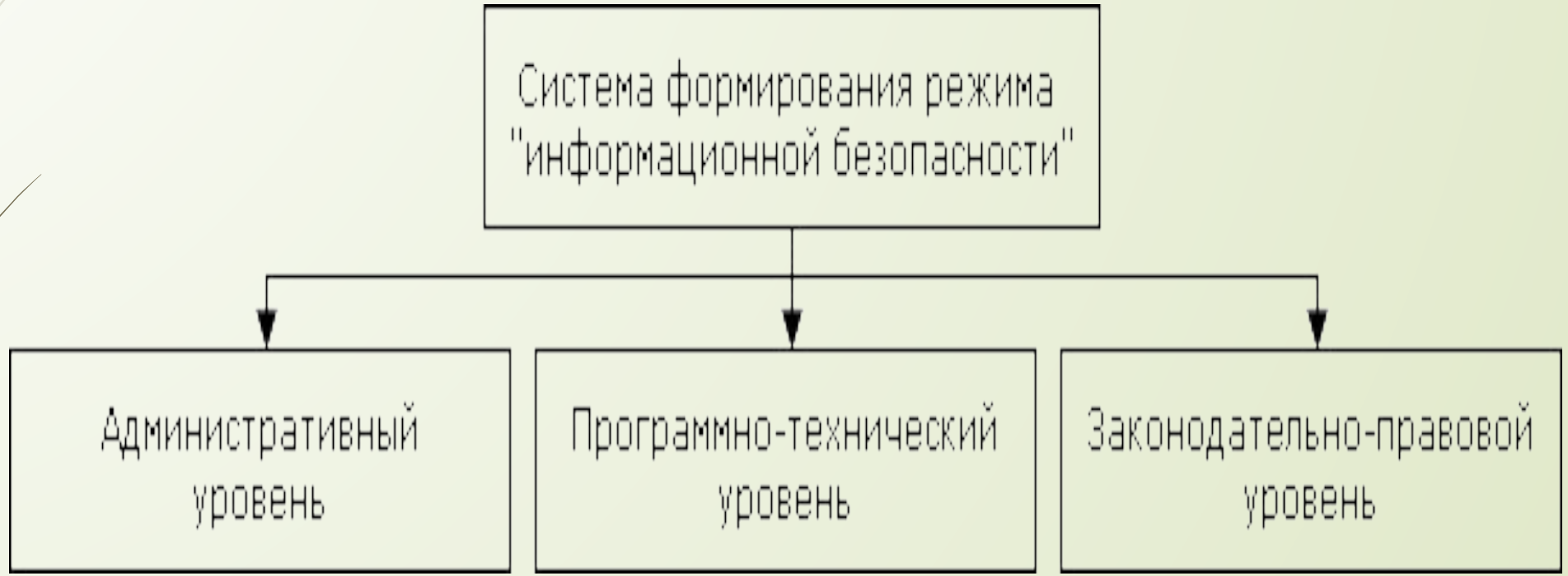
Основными задачами информационной безопасности в широком смысле являются

- защита государственной тайны, т. е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Задачи информационной безопасности

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

Уровни формирования режима информационной безопасности



- **Законодательно-правовой** уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний.

- **Административный уровень** включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации.
Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

- **Программно-технический уровень** включает три подуровня: *физический, технический (аппаратный)* и *программный*.

- **Физический** подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т. д.).

- Средства защиты **аппаратного** и **программного** подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д.

Домашнее задание

Описать любой объект с реализацией 3-х уровней обеспечения информационной безопасности.