**Прочитать и законспектировать лекцию**

**Тема: Понятие, сущность, значение и правовое регулирование режима секретности в органах внутренних дел**

В настоящее время теория и практика защиты государственной тайны и конфиденциальной информации находятся на таком этапе развития, когда количество накопленных знаний и опыта должно неизбежно перейти в новое качество. ***В этой связи будет уместным определиться, что подлежит защите и как защищать.***

В этом контексте проблема защиты государственной тайны и конфиденциальной информации приобретает двухуровневый характер.

*Первый* – обеспечение общества информационными ресурсами, которые составляют потенциал государства в условиях соперничества в информационной сфере.

*Второй* – создание систем защиты информационного потенциала страны, т.е. разработка и внедрение защищенных информационных технологий и систем с гарантированным уровнем обеспечения безопасности секретной информации.

***Система защиты государственной тайны и конфиденциальной информации призвана*** ограждать интересы государства, а также интересы имущественных прав собственников информационных ресурсов от недобросовестных владельцев и пользователей информационными ресурсами и информационными системами, от конкурентов, разведок иностранных государств и т.п.

***По общему правилу система защиты государственной тайны в органах внутренних дел предполагает:***

1)создание самостоятельных режимно-секретных подразделений по защите информации в органах внутренних дел;

2)систематическую организацию и проведение организационных, технических и иных мероприятий по защите средств вычислительной техники, автоматизированных систем, других технических средств и систем, а также проведение мероприятий по их аттестации и сертификации;

3)организацию и проведение технических и иных мероприятий по категорированию и защите секретной информации в выделенных помещениях должностных лиц и структурных подразделений;

4)выявление возможных внедренных на объекты и в технические средства электронных устройств перехвата информации и т.д.

***Основными целями защиты государственной тайны в органах внутренних дел являются:***

1)предотвращение утечки, хищения, утраты, искажения, подделки информации ограниченного доступа;

2)предотвращение угроз безопасности личности, общества и государства;

3)предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации ограниченного доступа;

4)защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;

5)сохранение государственной тайны и конфиденциальности документальной информации.

***Сегодня информационная инфраструктура, информационные ресурсы становятся ареной межгосударственной борьбы за мировое лидерство.*** Поэтому на государственном уровне защите подлежит любая документированная информация, неправомерное обращение к которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

***В соответствии с Федеральным законом Российской Федерации от 27.07.2006 года № 149-ФЗ (в редакции от19.12.20016 года № 442-ФЗ, с изменениями, вступившими в силу с 01.01.2017 года) «Об информации, информационных технологиях и о защите информации» режим защиты информации устанавливается:***

1)в отношении сведений, отнесенных к государственной тайне – уполномоченными органами на основании Закона Российской Федерации «О государственной тайне» от 21 июля 1993 г.;

2)в отношении конфиденциальной документированной информации – собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.;

3)в отношении персональных данных – специально уполномоченными на то подразделениями (службами) и должностными лицами на основании Федерального закона Российской Федерации «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и т.п.

***Компьютерная информация, только та, которая охраняется законом, также представляет собой разновидность документированной информации,*** зафиксированной на специальном машинном носителе или ЭВМ (системе ЭВМ, их сети).

***На сегодняшний день система защиты государственной тайны в органах внутренних дел должна отвечать следующим принципам:***

*1)принцип ограничения доступа к информации и их носителям.*Значение этого принципа очевидно. *Основные методы его реализации – это* семантические (криптографические) методы ограничения доступа к большей части информации и физические методы ограничения доступа к критическим информационным ресурсам (к зонам хранения ключевой информации, используемой в криптографических методах; к зонам, где обработка информации возможна только в открытом виде).

*2)Принцип минимальной ценности информации*. Он предписывает создавать информационные системы с наименьшим количеством секретной или конфиденциальной информации. В идеальном варианте основная масса информации должна иметь самый низкий статус безопасности и возможность пользования ею только в случае поступления запроса.

*3)Принцип персональной ответственности исполнителей или владельцев информации.*Выполнение этого принципа позволяет снизить вероятность угроз безопасности информации от несанкционированного доступа со стороны внутренних субъектов.

*4)Принцип тотальной, сквозной идентификации информационных пользователей.* Этот принцип определяет необходимость наличия уникальных идентификаторов пользователей у всех информационных систем.

*5)Принцип взаимного установления подлинности информационного пользователя.*Основным направлением распространения данного принципа является применение криптографических методов аутентификации, активизированных в рамках информационного процесса.

*6)Принцип функциональной полноты системы защиты информации.* Этот принцип определяет необходимость наличия у информационной системы определенных функций защиты (*например*, функций идентификации, аутентификации, физической защиты или шифрования).

Все эти принципы должны учитываться при разработке и создании защищенных информационных технологий и систем в ОВД.