

**ТЕМА 2.
ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ
ЗАЩИТЫ ИНФОРМАЦИИ**

Лекция 2/1.

**Нормативно-правовое
обеспечение информационной
безопасности в РФ**

ЛЕКЦИЯ 2/1
НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
РФ

1. ПРАВОВОЙ РЕЖИМ ИНФОРМАЦИИ.

2. ОРГАНЫ, ОБЕСПЕЧИВАЮЩИЕ
ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РФ.

В соответствии со статьей 17 ФЗ « О полиции» от 7 февраля 2011 года полиция:

1. Имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных о гражданах (далее - банки данных).

2. Формирование и ведение банков данных осуществляются в соответствии с требованиями, установленными законодательством Российской Федерации.

4. Полиция **обеспечивает защиту информации**, содержащейся в банках данных, от неправомерного и случайного доступа, уничтожения, копирования, распространения и иных неправомерных действий.

В самом общем виде **«правовой режим информации»** следует понимать как совокупность норм, определяющих:

- права собственности, владения и распоряжения информацией;
- степень открытости информации, необходимость или возможность ее отнесения к категории ограниченного доступа;
- порядок отнесения информации к категории ограниченного доступа и уполномоченных на это лиц;
- порядок документирования, доступа, хранения, контроля и распространения информации;
- применение различных средств и методов обеспечения информационной безопасности;
- порядок привлечения к ответственности и меры наказания за нарушение установленных норм и правил в области информационных отношений.

Акты федерального законодательства

- Конституция РФ;
- Международные договора;
- Федеральные законы;
- Указы Президента РФ;
- Постановления правительства РФ.

Нормативные документы государственных органов РФ:

- Доктрина информационной безопасности РФ;
- Руководящие документы ФСТЭК;
- Приказы ФСБ;

Стандарты информационной безопасности:

- **Международные стандарты;**
- **Государственные (национальные) стандарты РФ;**
- **Рекомендации по стандартизации;**
- **Методические указания.**

наиболее важным сегодня следует отнести следующие нормативно-правовые акты федерального законодательства:

- закон «О государственной тайне» от 21.07.93 г. № 5485-1;
- закон «Об обязательном экземпляре документов» от 29.12.94. № 77;
- закон «Об архивном деле в Российской Федерации» от 22.10.04. № 125;
- закон «О коммерческой тайне» от 29.07.04. № 98;
- закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 г. № 149;
- закон «О персональных данных» от 27.07.06 №152;
- закон «Об электронной подписи» от 06.04.11 № 63.

Для обеспечения применения к информации норм вещного права вводится понятие *документированная информация* - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель

При решении организационно-правовых вопросов обеспечения информационной безопасности исходят из того, что информация подпадает под нормы **вещного права**, это дает возможность применять к информации нормы уголовного и гражданского права в полном объеме.

В ст. 2 п.5 закон «Об информации, информационных технологиях и о защите информации» введено понятие *обладателя информации* в информационной области. Обладатель информации вправе:

- ⦿ разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- ⦿ использовать информацию, в том числе распространять ее по своему усмотрению;
- ⦿ передавать информацию другим лицам по договору или на ином установленном законом основании;
- ⦿ защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами.

Авторское право (право интеллектуальной собственности) как самостоятельный институт решает конкретные задачи, которые включают всемирную охрану:

- 1.имущественных, личных неимущественных прав и законных интересов авторов;
- 2.обеспечение правовыми средствами наиболее благоприятных условий для создания научных и художественных произведений;
- 3.широкое использование их обществом.

Авторское право
распространяется на любые
программы для компьютеров и
базы данных, как выпущенные,
так и не выпущенные в свет,
представленные в объективной
форме независимо от
материального носителя.

В общем случае информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- 1) информацию свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Свободно распространяемая информация

В соответствии со ст.8 п.4 законом «Об информации, информационных технологиях и о защите информации» не может быть ограничен доступ к:

- 1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- 2) информации о состоянии окружающей среды;
- 3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- 4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- 5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Ограничение доступа к информации

Ограничение доступа обязательно для информации, доступ к которой ограничен федеральными законами; они же устанавливают условия отнесения информации к сведениям, составляющим коммерческую, служебную и иную тайну.

Если информация получена гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), она подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Правовой режим защиты информации ограниченного доступа



ГОСУДАРСТВЕННАЯ ТАЙНА

К ним отнесены сведения (указаны лишь разделы):

- в военной области;
- о внешнеполитической и внешнеэкономической деятельности;
- в области экономики, науки и техники;
- в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

В зависимости от вида, содержания и размеров ущерба можно выделить **группы некоторых видов ущерба** при утечке (или возможной утечке) сведений, составляющих государственную тайну.

1. Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации, утрата страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т. д.

2. Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т.д. Экономический ущерб может быть выражен, прежде всего в денежном исчислении.

К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

- в порядке, установленном Гражданским кодексом Российской Федерации, введенным в действие с 1995 года, предусмотрена категория **«служебная тайна»**, **«коммерческая тайна»**, **«персональные данные»**

- Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (**персональные данные**), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
- Сведения, составляющие тайну следствия и судопроизводства (**процессуальная тайна**).
- Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (**служебная тайна**).
- Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее (**профессиональная тайна**)).
- Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (**коммерческая тайна**).
- Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

ВОПРОС 2. ОРГАНЫ (ПОДРАЗДЕЛЕНИЯ), ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

В зависимости от деятельности в области защиты информации (в рамках государственных органов власти или коммерческих организаций), сама деятельность организуется специальными государственными органами (подразделениями), либо отделами (службами) предприятия.

ГОСУДАРСТВЕННЫЕ ОРГАНЫ РФ, КОНТРОЛИРУЮЩИЕ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ:

- ◎ Совет безопасности России
- ◎ Федеральная служба по техническому и экспортному контролю
- ◎ Федеральная служба безопасности
- ◎ Министерство внутренних дел РФ
- ◎ Федеральная служба охраны
- ◎ Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия
- ◎ Межведомственная комиссия по защите государственной тайны

СЛУЖБЫ, ОРГАНИЗУЮЩИЕ ЗАЩИТУ ИНФОРМАЦИИ НА УРОВНЕ ПРЕДПРИЯТИЯ:

- Служба экономической безопасности
 - Служба безопасности персонала
 - Отдел кадров
 - Служба информационной безопасности
-

СОВЕТ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

- ⦿ Правовую основу деятельности Совета Безопасности составляют **Конституция** Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, **Федеральный закон** от 28 декабря 2010 г. № 390-ФЗ «О безопасности», другие федеральные законы, указы и распоряжения Президента Российской Федерации.
- ⦿ Совет Безопасности формируется и возглавляется Президентом Российской Федерации.

Основными функциями Совета Безопасности являются:

- 1) рассмотрение вопросов обеспечения безопасности,, военно-технического сотрудничества Российской Федерации с иностранными государствами, иных вопросов, связанных с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также вопросов международного сотрудничества в области обеспечения безопасности;
- 2) анализ информации о реализации основных направлений государственной политики в области обеспечения безопасности, о социально-политической и об экономической ситуации в стране, о соблюдении прав и свобод человека и гражданина;

- 3) разработка и уточнение стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов, а также критериев и показателей обеспечения национальной безопасности;
- 4) осуществление стратегического планирования в области обеспечения безопасности;
- 5) рассмотрение проектов законодательных и иных нормативных правовых актов Российской Федерации по вопросам, отнесенным к ведению Совета Безопасности;
- 6) подготовка проектов нормативных правовых актов Президента Российской Федерации по вопросам обеспечения безопасности и осуществления контроля деятельности федеральных органов исполнительной власти в области обеспечения безопасности и т.д

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) создана в соответствии с Указом Президента Российской Федерации от 09 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» вместо существовавшей ранее Государственной технической комиссии при Президенте Российской Федерации и является головным органом по защите информации. Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации. ФСТЭК России подведомственна Минобороны России.

ФСТЭК России :

- 1) обеспечения безопасности (*некриптографическими методами*) информации в системах информационной и телекоммуникационной инфраструктуры, информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
- 2) противодействия иностранным техническим разведкам на территории Российской Федерации;
- 3) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- 4) осуществления экспортного контроля.

В Российской Федерации коммерческая деятельность, связанная с использованием **криптографических средств**, подлежит обязательному лицензированию.

С 22 января 2008 года действует постановление Правительства РФ от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами», которым приняты

Положения о лицензировании деятельности по:

- распространению шифровальных (криптографических) средств;
- техническому обслуживанию шифровальных (криптографических) средств;
- предоставлению услуг в области шифрования информации;
- разработке, производству шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Федеральная служба безопасности.

Обеспечение информационной безопасности — деятельность органов ФСБ, осуществляемая ими в пределах своих полномочий:

1. формирует и реализует государственную политику в области обеспечения информационной безопасности с использованием инженерно-технических и криптографических средств;
2. обеспечивает криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационные системы, а также системы шифрования, и иные виды специальной связи в России и её учреждениях, а так же за ее пределами.

Для достижения указанной цели федеральными органами **ФСТЭК** и **ФСБ** решаются следующие задачи технического контроля:

- оценка достаточности и эффективности организационных и технических мероприятий по защите информации от утечки по техническим каналам;
- проверка эффективности защиты информации от утечки по отдельным физическим полям и соответствующим типам аппаратуры съема и перехвата информационных сигналов;
- определение зон возможного перехвата информации техническими средствами и др

Межведомственная комиссия по защите государственной тайны

осуществляет следующие основные полномочия в области информационной безопасности:

- 1) координирует деятельность органов государственной власти, органов местного самоуправления и организаций по вопросам реализации федерального законодательства в области государственной тайны;
- 2) рассматривает и представляет в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации предложения по правовому регулированию вопросов защиты государственной тайны и совершенствованию системы защиты государственной тайны в Российской Федерации, а также предложения по организации разработки и выполнения государственных программ, нормативных правовых актов и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне;

- 3) формирует перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне;
- 4) формирует перечень сведений, отнесенных к государственной тайне;
- 5) формирует в установленном порядке перечень особорежимных объектов Российской Федерации и представляет его в Правительство Российской Федерации;
- 6) определяет порядок рассекречивания носителей сведений, составляющих государственную тайну;
- 7) рассматривает вопросы о возможности передачи сведений, составляющих государственную тайну, другим государствам и международным организациям и представляет в установленном порядке в Правительство Российской Федерации соответствующие экспертные заключения;
- 8) координирует в установленном порядке проведение работ по лицензированию деятельности организаций, связанной с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны и т.д.

Контрольные вопросы

1. Назовите информационно-правовые нормы Конституции РФ.
2. Перечислите службы образующие государственную систему защиты информации.
3. Назовите основные задачи, которые ставит перед собой служба технического контроля.
4. Дайте понятие правового режима информации.
5. Назовите информацию, которая в соответствии с законодательством РФ относится к авторскому праву.
6. Назовите основные причины утечки информации.
7. Перечислите каналы утечки информации применительно к АС

ЛИТЕРАТУРА

- ⦿ Аполлонский А.В., Домбровская Л.А., Примакин А.И., Смирнова О.Г., Основы информационной безопасности в ОВД: Учебник для вузов. – СПб.: Университет МВД РФ, 2010 – 174 с.
- ⦿ Доценко С.М., Примакин А.И. Информационная безопасность и применение информационных технологий в борьбе с преступностью: Учебник для вузов. – СПб.: Университет МВД РФ, 2004 – С. 10-30, С. 84-107, С. 113-145.
- ⦿ Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. Фонд «Университет». СПб 2000. - 428 с.