

Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

ВВЕДЕНИЕ

Цель, задачи и содержание курса

1. Объект защиты

Применять средства защиты информации можно только к физическим объектам, поэтому защищаются материальные носители информации:

- персонал,
- документы,
- технические средства.

2. Средства защиты

В основе комплексной системы защиты лежат следующие методы защиты:

правовые , организационные и технические.

Методы защиты информации

Правовые

-Международное право
-Государственные, местные, ведомственные, внутрифирменные правовые акты

Организационные

-Создание СБ
-Введение режима ЗИ
-Подготовка и переподготовка кадров
-Системы лицензирования и сертификации в области ЗИ

Технические

-Программные, аппаратные
-Криптографические средства
-Физические препятствия

Цель курса:

Получение необходимых знаний по организационно-правовым вопросам защиты информации юридических и физических лиц.

Задачи курса:

- знакомство с действующей в РФ законодательной базой в области ЗИ;
- получение знаний о применении организационных и технических методов защиты экономической информации на предприятии;
- выработка умения самостоятельно анализировать содержание законодательных актов и эффективно применять методы защиты информации.

Содержание курса

- 1. Структура и состав информационного законодательства**
- 2. Правовые основы пользования информационными ресурсами**
- 3. Защита информации ограниченного доступа**
- 4. Основы использования организационных методов защиты информации**
- 5. Основы использования технических методов защиты информации**
- 6. Лицензирование и сертификация в области ЗИ**
- 7. Система юридической ответственности за нарушение норм ЗИ**
- 8. Защита интеллектуальной собственности**
- 9. Нормативные документы в области защиты от киберпреступлений**

**Всего по плану семестра аудиторных занятий 54 часа, в том числе лекции и практические работы (компьютерные тесты).
По окончании – экзамен**

Учебная и учебно-методическая литература

1. Копылов В.А. Информационное право: Учебное пособие. - М.: Юристъ, 2003. – 512.
2. **Городов О.А.** Информационное право: Учебник. - М.: ТК Велби, Изд-во Проспект, 2007. – 248 с.
3. **Ярочкин В.И.** Система безопасности фирмы. - М.: Ось-89, 1997.
4. **Вехов В.Е.** Компьютерные преступления: Способы совершения и раскрытия. - М.: Право и Закон, 1996.
5. **Шаваев А.Г.** Криминологическая безопасность негосударственных объектов экономики. - М.: ИНФРА-М, 1995.
6. **Струков В.И.** Правовое обеспечение защиты информации. Методическое пособие, часть 1 и 2. (№4196) и (№4196-2).
7. **Электронный учебник** по курсу ПОИБ.
8. **Струков В.И.** Презентации лекций по курсу ОПОИБ.
9. **Струков В.И.** Методические указания к выполнению лабораторных работ (№3563).

Периодические издания

Журналы: «Защита информации» - Инсайд; БИТ, БДИ и др.

Правовые документы

- 1. Закон РФ “Об информации, информационных технологиях и о защите информации” от 27.07.2006г. № 149-ФЗ.**
- 2. Закон РФ “О государственной тайне” от 21.07.93г. №5485-1 (ред. 11.11.2003г. №153).**
- 3. Закон РФ “О коммерческой тайне”, от 29.07.2004г. №98-ФЗ.**
- 4. Закон РФ “О персональных данных” от 27.07.2006 г. N 152-ФЗ.**
- 5. Закон РФ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ**
- 6. Закон РФ “Об архивном деле в РФ” от 22.10.2004 г. №125-ФЗ.**
- 7. Закон РФ “О федеральной фельдъегерской связи” от 17.12.1994г. № 67-ФЗ (ред. от 20.04.2006 г.).**
- 8. Гражданский кодекс РФ, Уголовный кодекс РФ и др. кодексы.**
- 9. Закон РФ “О лицензировании отдельных видов деятельности”, от 8.08.2001г. №128 (ред. от 4 мая 2011 г. N 99-ФЗ).**

Тема 1

Структура и состав информационного законодательства

1.1. Нормативно-правовое регулирование общественных отношений

Нормативно-правовое регулирование отношений в области защиты информации осуществляется **информационным правом**, которое является одним из составляющих существующей **системы права**.

В юриспруденции представлены много таких составляющих, которых объединяет одна общая научная дисциплина - **теория государства и права**. Она изучает закономерности возникновения, развития, назначения и функционирования государства и права.

Основы этих знаний рассматриваются в курсе «Правоведение».

(**Самостоятельно повторить разделы: Структура правового отношения; Юридическая ответственность; Состав правонарушения.**)

Классификация нормативно-правовых актов.

По юридической силе.

По субъектам, их издающим.

По субъектам их издающим правовые акты подразделяются на

акты законодательной власти (законы);

акты исполнительной власти (подзаконные акты);

акты судебной власти (юрисдикционные акты общего характера).

По юридической силе все нормативно-правовые акты подразделяются на

законы,

подзаконные акты.

Признаки закона :

-законы принимаются высшими законодательными органами государства
(Федеральное собрание – Государственная Дума и Совет Федерации) ;

-принятие закона включает в себя четыре обязательные стадии:

- внесение законопроекта в законодательный орган;
- обсуждение законопроекта;
- принятие закона;
- его опубликование в течении 7 дней после подписания Президентом.

(Неопубликованные законы не применяются. Конституция ст. 15).

Законы вступают в силу по истечении 10 дней после их опубликования,

-законы не подлежат контролю или утверждению со стороны какого-либо другого органа государства. Они могут быть отменены или изменены только законодательной властью. Конституционный или другой аналогичный суд может признать закон, принятый парламентом, неконституционным, однако отменить его может только законодательный орган.

Подзаконные нормативно-правовые акты подразделяются на

Указы президента. В системе подзаконных актов они обладают высшей юридической силой и издаются на основе и в развитие законов (вступают в силу по истечении 7 дней после их опубликования).

Постановления правительства. Это подзаконные нормативные акты, принимаемые в контексте с указами президента (вступают в силу по истечении 7 дней после их опубликования).

Местные акты. Это нормативно-правовые акты органов законодательной и исполнительной власти на местах. Действие этих актов ограничено подвластной им территорией.

Ведомственные (приказы, инструкции). Это нормативно-правовые акты общего действия, однако они распространяются лишь на ограниченную сферу общественных отношений (таможенные, банковские, транспортные, государственно-кредитные и другие).

Внутриорганизационные. Это такие нормативно-правовые акты, которые издаются различными организациями для регламентации своих внутренних вопросов и распространяются на членов этих организаций.

Иерархия правовых актов РФ

Конституция РФ

Федеральные конституционные законы РФ

Федеральные законы РФ

Указы и распоряжения Президента РФ

Законодательные акты субъектов РФ

**Постановления и распоряжения
Правительства РФ**

**Нормативные правовые акты
федеральных органов
исполнительной власти**

Правовые акты органов местного самоуправления

**Нормативные правовые акты высших
органов исполнительной власти
субъектов РФ**

**Нормативные правовые акты органов
исполнительной власти
субъектов РФ**

Юридическая ответственность подразделяется по отраслевому признаку:

Уголовная ответственность наступает за совершение преступлений и устанавливается только уголовным законом.

Административно-правовая ответственность наступает за совершение административных проступков. Меры административного принуждения - предупреждение, штраф, лишение специального права, административный арест.

Гражданско-правовая ответственность наступает за нарушения договорных обязательств имущественного характера или за причинение имущественного внедоговорного вреда. (Возмещение убытков, выплата неустойки).

Дисциплинарная ответственность возникает вследствие совершения дисциплинарных проступков. Меры дисциплинарной ответственности - выговор, строгий выговор, отстранение от занимаемой должности и т.п.

Материальная ответственность рабочих и служащих за ущерб, нанесенный предприятию, учреждению. Размер возмещаемого ущерба определяется в процентах к заработной плате (1/3, 2/3 месячного заработка).

1.2. Система и строение права

Система права это совокупность всех нормативно-правовых актов.

Внутреннее строение права можно представить по вертикали и горизонтали.

Вертикальное строение права - это совокупность следующих элементов:

Отрасль права - охватывает сферу общественных отношений. *Например, имущественные отношения - гражданское право, управленческие отношения - административное право, и т.п.*

Подотрасль права - охватывает **область** общественных отношений. Многие отрасли права имеют подотрасли. *Например, в гражданском праве выделяются подотрасли - авторское и наследственное право.*

Институт права - охватывает **вид** общественных отношений. *В трудовом праве - институт трудового договора.*

Субинститут права - охватывает **разновидность** общественных отношений. *Институт преступлений против жизни, здоровья, достоинства личности делится на субинституты преступлений против жизни, против здоровья и преступлений против достоинства личности.*

Норма права - это обязательное правило поведения, охраняемое силой государственного принуждения.

Правовое предписание - это часть нормы права, логически завершенная и обособленная. *Размер алиментов, взыскиемых на одного ребенка (25 % заработка), на двух (33 %), на трех и более (50 %).*

Горизонтальное строение права показывает все отрасли, его составляющие.

Выделяют две группы отраслей **регулятивные и охранительные**.

Регулятивные отрасли устанавливают права и обязанности участников правоотношений. Это следующие отрасли:

- **конституционное право** закрепляет основы государственного и общественного строя страны.

Главным нормативным актом отрасли является Конституция;

- **административное право** регулирует общественные отношения, возникающие в процессе исполнительно-распорядительной деятельности органов государства;

- **гражданское право** регулирует различные имущественные отношения.
Основной нормативный акт - Гражданский кодекс (ГК);

- **финансовое право** регулирует доходы и расходы государства.

Основные акты: Федеральный закон о государственном бюджете, законы о налогах;

- **банковское право.** Создание банков, принципы их деятельности, и т.д. *регулирует Закон о банках и банковской деятельности;*

Регулятивные отрасли (продолжение)

- **предпринимательское право** регулирует экономические рыночные отношения. *Основные нормативные акты - ГК, Законы об АО и ООО;*
- **трудовое право** регулирует общественные отношения, связанные с применением труда. *Основной нормативный акт – Трудовой Кодекс (ТК);*
- **природоресурсное право** определяет порядок владения, пользования и распоряжения природными ресурсами: землей (*Земельный кодекс*), недрами (*Закон о недрах*), водой (*Водный кодекс*), воздушным пространством (*Воздушный кодекс*), лесными богатствами (*Лесной кодекс*);
- **экологическое право** регулирует защиту природных объектов и всей окружающей среды. Нормы экологического права рассредоточены по многим нормативным актам (*УК, КоАП, ГК и др.*);
- **информационное право** регулирует комплекс общественных отношений, связанных с информацией, защитой информации, защитой прав собственников информационных ресурсов, формирования различных институтов тайн (*государственной, служебной, банковской, коммерческой, личной и т.п.*).

Охранительные отрасли права (защита правоотношений):

- **уголовное право** – устанавливает общественно опасные деяния (преступления) и наказание за их совершение.

Основной нормативный документ - Уголовный кодекс (УК);

- **уголовно-процессуальное право** объединяет нормы, определяющие порядок проведения предварительного следствия, дознания, порядок ведения судебного разбирательства, назначения наказания.

Основной нормативный акт - Уголовно-процессуальный кодекс (УПК);

- **уголовно-исполнительное право** регулирует процесс исполнения мер уголовного наказания.

Основной нормативный акт - Уголовно-исполнительный кодекс (УИК);

- **гражданско-процессуальное право** регулирует порядок рассмотрения споров (трудовые, жилищные, наследственные и др.), в которых хотя бы одной из сторон выступает гражданин.

Основной нормативный акт - Гражданский процессуальный кодекс;

- **арбитражно-процессуальное право** регулирует порядок рассмотрения гражданско-правовых споров между юридическими лицами.

Основной нормативный акт - Арбитражно-процессуальный кодекс.

Международное право –

система норм, регулирующих отношения между государствами

- международное публичное право

и государства с иностранными лицами

- международное частное право.

1.3. Структура информационного законодательства

Первые правовые документы в области информационного права в России, с которых началось формирование информационного законодательства:

“Концепция правовой информатизации России”

утверждена Указом Президента РФ от 28.06.93 г. №966.

Гражданский кодекса РФ принят в 1994г.

Закон РФ “Об информации, информатизации и защите информации” принят в 1995г.

Сравнение свойств материального объекта и информации

Свойства обычного товара

Цена

Потребительские свойства

Жизненный цикл товара (ЖЦТ)

Свойства информации

Цена

Потребительские свойства

Жизненный цикл информации

Нематериальность

Неисчерпаемость

Сохраняемость

Информационное законодательство - это совокупность норм права, регулирующих общественные отношения в информационной сфере.

Предмет правового регулирования в информационной сфере:

- создание и распространение информации;
- формирование информационных ресурсов;
- реализация права на поиск, получение, передачу и потребление информации;
- создание и применение информационных систем и технологий;
- создание и применение средств информационной безопасности.

Структура информационного законодательства РФ.

Международные акты информационного законодательства, начиная с Всеобщей декларации прав человека от 10.12.1948г.

Конституция РФ

Гражданский кодекс РФ, Уголовный кодекс РФ и др. кодексы.

Законы РФ:

**“Об информации, информационных технологиях и о защите информации”, “О государственной тайне”, “О коммерческой тайне”, “О персональных данных”, “Об электронной подписи”
и др.**

(всего около 80 законов)

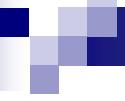
**Указы и Распоряжения Президента РФ. Постановления
Правительства РФ.**

**Местные, ведомственные и внутриорганизационные подзаконные
акты.**

**Совокупность вышеперечисленных документов составляет правовую
базу в информационной сфере.**

Контрольные вопросы

- 1. Цель изучения курса «Организационное и правовое обеспечение информационной безопасности».**
- 2. Какие методы используются при создании комплексной системы информационной безопасности объекта?**
- 3. Классификация нормативно-правовых актов.**
- 4. Юридическая ответственность за нарушения правовых норм.**
- 5. Место информационного права в системе права.**
- 6. Назовите свойства информационного товара.**
- 7. Что является предметом правового регулирования в информационной сфере?**
- 8. Какова структура информационного законодательства в РФ?**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы по теме 1

- 1. Цели и задачи изучения курса «Организационная и правовая защита информации».**
- 2. Классификация нормативно-правовых актов.**
- 3. Юридическая ответственность за нарушения правовых.**
- 4. Место информационного права в системе права.**
- 5. Назовите свойства информационного товара.**
- 6. Что является предметом правового регулирования в информационной сфере?**
- 7. Какова структура информационного законодательства в РФ?**

2. Правовые основы пользования информационными ресурсами

2.1. Основные определения в области информационного права

**В состав информационного законодательства в настоящее время входят
следующие документы:**

Международные акты информационного законодательства

Конституция РФ

Гражданский, Уголовный, Трудовой и др. Кодексы

Законы РФ:

“Об информации, информационных технологиях и о защите информации”,
“Об обязательном экземпляре документов”, “О государственной тайне”,
“О средствах массовой информации”, “О связи”, “Об архивном деле в РФ”,
“Об электронной подписи”, “О коммерческой тайне”, “О рекламе”,
“О персональных данных”, “О библиотечном деле”,
“О почтовой связи”, “О федеральной фельдъегерской связи”,
“О банках и банковской деятельности” и др. законы.

Подзаконные акты:

Указы и Распоряжения Президента РФ,

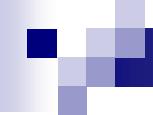
**Постановления Правительства РФ, местные, ведомственные
и внутриорганизационные акты.**

Основной нормативно-правовой документ в сфере информационного права

**Закон РФ “Об информации, информационных технологиях
и о защите информации” от 27.13.2006г. № 149-ФЗ**

регулирует следующие отношения:

- осуществление права на поиск, получение, передачу, производство и распространение информации;**
- ограничение доступа к информации;**
- применение информационных технологий.**



В законе раскрыты следующие важные вопросы:

- 1. Основные понятия в области информации, и ее защиты.**
- 2. Права обладателя информации.**
- 3. Право на доступ и ограничения доступа к информации.**
- 4. Использование информационно-телеkomмуникационных сетей и государственное регулирование в этой сфере.**
- 5. Защита информации, в том числе использование ЭЦП.**

В законе даны определения:

информация - сведения (сообщения, данные) независимо от формы их представления (может являться объектом правовых отношений и свободно использоваться любым лицом за исключением ограничений, введенных законом);

конфиденциальность информации - обязательное требование не передавать такую информацию третьим лицам без согласия ее обладателя;

документированная информация - зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления и распространения информации;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

информационная система - совокупность:

информации, содержащейся в базах данных;

информационных технологий, обрабатывающих информацию;

технических средств обеспечивающих обработку информации.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются **государственными информационными ресурсами**.

Электронное сообщение, подписанное электронной цифровой подписью, признается, равнозначным документу, подписанному собственноручной подписью.

Защита информации представляет собой принятие
правовых, организационных и технических мер,

направленных на:

**обеспечение защиты информации от неправомерного доступа,
уничтожения, модификации, блокирования, копирования,
предоставления, распространения, а также от иных
неправомерных действий в отношении такой информации;**

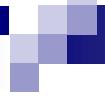
**соблюдение конфиденциальности информации ограниченного
доступа,**

реализацию права на доступ к информации.

Принципы

правового регулирования отношений в информационной сфере

- 1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;**
- 2) установление ограничений доступа к информации только федеральными законами;**
- 3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации;**
- 4) обеспечение безопасности Российской Федерации при создании и эксплуатации информационных систем;**
- 5) достоверность информации и своевременность ее предоставления;**
- 6) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;**
- 7) недопустимость преимуществ применения одних информационных технологий перед другими, кроме государственных информационных систем установленных в соответствии с федеральными законами.**



Информационную безопасность в России обеспечивают:

Правительство РФ, Совет безопасности РФ,

Федеральная служба безопасности РФ (ФСБ),

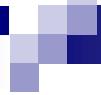
Служба специальной связи и информации при Федеральной службе охраны РФ,

Федеральная служба по техническому и экспортному контролю РФ (ФСТЭК) (бывшая ГТК),

Государственная фельдъегерская служба РФ,

Межведомственная комиссия по защите государственной тайны.

Требования о защите информации, в государственных информационных системах, устанавливаются уполномоченным федеральным органом исполнительной власти.



Нарушение требований настоящего Федерального закона влечет за собой ответственность:
дисциплинарную,
гражданско-правовую,
административную
или уголовную
в соответствии с законодательством Российской Федерации.

Лица, права которых были нарушены, вправе обратиться за судебной защитой своих прав (суд, суд третейский, суд арбитражный).

Кроме защиты информации необходима защита от информации (от вредной информации).

2.2. Права обладателя и режимы доступа к информации

Обладателем информации может быть физическое лицо, юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

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.**

**Информация (зависимости от порядка распространения)
подразделяется на:**

- свободно распространяемую;**
- предоставляемую по соглашению;**
- распространяемую в соответствии с федеральными
законами;**
- распространение которой в РФ ограничивается или
запрещается.**

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

В законе определены режимы информации свободного и ограниченного доступа.

Режимы доступа к информации

в соответствии с Законом РФ “Об информации, информационных технологиях и о защите информации” от 27.07.2006г. № 149-ФЗ и Указом Президента РФ № 188 от 6.03.1997г.

Режим доступа	Вид режима	Состав сведений
Свободный доступ	Общественного достояния	Научные открытия, рукописи и т.п.
	Массовой информации	Информация в СМИ, различные публикации и т.д.
	Исключительных прав	Результаты интеллектуальной деятельности
Ограниченный доступ	Конфиденциальности	Коммерческая, служебная и профессиональная тайны. Персональные данные. Тайна следствия и судопроизводства. Сведения о сущности неопубликованных изобретений
	Государственной тайны	Секретно, совершенно секретно и особой важности

Режим исключительных прав (защита объектов интеллектуальной собственности)

Существует три общепризнанные в мире правовые формы защиты интеллектуальной собственности:

авторское право,

патентное право,

и секреты производства - «ноу-хау».

Режим исключительных прав определен

Гражданским кодексом РФ, часть 4, от 18.12.2006г. № 230.

Режим общественного достояния

Создает условия для беспрепятственного ознакомления и использования соответствующих сведений

Так истечение срока действия исключительных прав на объекты интеллектуальной собственности

(например, **авторское право** действует в течении всей жизни автора и **70 лет** после его смерти)

означает переход их в общественное достояние

Произведение, перешедшее в общественное достояние, может свободно использоваться любым лицом без чьего-либо согласия или разрешения и без выплаты авторского вознаграждения.

При этом охраняются авторство, имя автора и неприкосновенность произведения. (ГК РФ часть 4, ст. 1282)

Режим массовой информации

Распространяется на информацию в СМИ и различные публикации и отражает гарантированную Конституцией РФ свободу массовой информации (ст. 29).

Ограничения на публикуемые в СМИ сообщения даны в
Конституции РФ

Законе РФ «О средствах массовой информации» от 27 декабря 1991 года № 2124-1, (ред. от 16.10.2006 №160-ФЗ).

Режим ограниченного доступа

включает режим государственной тайны и режим конфиденциальности

Режим государственной тайны

устанавливается в соответствии с законом РФ “О государственной тайне”.

Режим конфиденциальности

устанавливается в отношении сведений, перечисленных в Указе Президента РФ № 188 от 6.03.1997г. (ред. от 23.09.2005 №1111) и регулируется законами:

“О коммерческой тайне”, “О персональных данных”, “О связи”, “О банках и банковской деятельности”, “О полиции” и др.

Режим конфиденциальной информации по данным законодательных и подзаконных актов в настоящее время включает более 50 видов тайн.

Указом Президента РФ № 188 от 6.03.1997г. утвержден перечень сведений конфиденциального характера:

Коммерческая тайна

Служебная тайна

Профессиональная тайна

Персональные данные

Тайна следствия и судопроизводства

Сведения о сущности неопубликованных изобретений

**В отношении профессиональной тайны
действуют нормы Закона “Об информации, информационных
технологиях и о защите информации” (статья 9)**

Профессиональная тайна - информация, полученная лицами при исполнении ими профессиональных обязанностей, подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Профессиональная тайна, может быть предоставлена третьим лицам в соответствии с федеральными законами или по решению суда.

Срок сохранения профессиональной тайны, может быть ограничен только с согласия гражданина, предоставившего такую информацию о себе.

Правовое регулирование персональных данных

Отношения, связанные с обработкой персональных данных, осуществляющей органами государственной власти, юридическими и физическими лицами регулируются Законом РФ

“О персональных данных” от 27.07.2006 г. № 152-ФЗ.

В законе дается различие **общедоступных и конфиденциальных** персональных данных (ст. 3):

-конфиденциальность персональных данных - обязательное требование не допускать их распространение без согласия субъекта персональных данных или законного основания;

-общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или в соответствии с федеральными законами.

Правовое регулирование служебной тайны

Определение понятия «служебная тайна» дано в 1 части ГК РФ, в ст.139 **“Служебная и коммерческая тайна”:**

-информация составляет **служебную или коммерческую** тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

В отличии от **профессиональной** тайны **служебная** тайна связана с интересами государственной службы и службы в органах местного самоуправления.

Нормативно-правовыми документами в отношении защиты служебной тайны являются:

Закон РФ “Об основах государственной службы РФ” от 31.07.95 №119-ФЗ.

Закон РФ “О прокуратуре РФ” от 17.01.92 №2202-1 (ред. от 10.02.99).

Закон РФ “О банках и банковской деятельности” от 02.12.90 №395-1 (ред. от 31.07.98 №151).

Закон РФ “О полиции” от 07.02.2011.№3 -ФЗ.

Закон РФ “Об оперативно-розыскной деятельности” от 12.08.95г. №144-ФЗ.

Закон РФ “О связи” от 16.02.95 №15-ФЗ (ред. от 06.01.99).

Закон РФ “О коммерческой тайне” от 29.07.2004г. №98-ФЗ.

Государственное регулирование в сфере применения информационных технологий

В ст. 12 закона об информации говорится о необходимости создания условий для эффективного использования в Российской Федерации

**информационно-телекоммуникационных сетей,
в том числе сети "Интернет",**

но при этом делаются следующие ограничения.

При использовании информационно-телекоммуникационных сетей, передача информации осуществляется без ограничений при условии (ст. 15)

**соблюдения требований к распространению информации
и
охране объектов интеллектуальной собственности.**

В ст. 15 закона “Об информации...” установлены нормы защиты прав пользователя информационными сетями

При использовании почтовых отправлений и электронных сообщений, **отправитель информации обязан обеспечить получателю возможность отказа от такой информации.**

Федеральными законами может быть **предусмотрена обязательная идентификация лиц, использующих информационно-телекоммуникационную сеть.**

При этом получатель электронного сообщения вправе установить **отправителя электронного сообщения.**

Дополнения в закон «Об информации» от 5 мая 2014 г. N 97-ФЗ.
Введено понятие:

Единая система идентификации и аутентификации -
федеральная государственная информационная система,
которая обеспечивает в случаях, предусмотренных
законодательством РФ, санкционированный доступ к
информации, содержащейся в информационных
системах.

Добавлены статьи:

**Статья 15.2. Порядок ограничения доступа к информации,
распространяемой с нарушением исключительных
прав на фильмы, в том числе кинофильмы,
телефильмы**



Статья 10.1. Обязанности организатора распространения информации в сети "Интернет"

Устанавливает требования:

Организатор распространения информации в сети "Интернет" обязан обеспечивать реализацию требований к оборудованию и программно-техническим средствам, используемым им в эксплуатируемых информационных системах, для проведения органами, осуществляющими ОРД, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий.

"Статья 13.31. Неисполнение обязанностей организатором распространения информации в сети "Интернет "

2. Неисполнение организатором распространения информации в сети "Интернет" установленной федеральным законом обязанности хранить и (или) предоставлять уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети "Интернет" и информацию о таких пользователях -

влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от трехсот тысяч до пятисот тысяч рублей.

3. Неисполнение организатором распространения информации в сети "Интернет" обязанности обеспечивать реализацию установленных в соответствии с ФЗ требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности РФ, в случаях, установленных федеральными законами, мероприятий в целях осуществления таких видов деятельности, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий -

влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от трехсот тысяч до пятисот тысяч рублей.

Правила использования информационно-телекоммуникационных сетей даны также в Указе Президента РФ от 12.05.2004 N611:

1. Субъектам международного информационного обмена в РФ **не осуществлять включение информационных систем**, сетей, в которых обрабатывается информация, **содержащая государственную тайну**, и служебная информация ограниченного распространения в состав средств международного информационного обмена, в том числе в «Интернет».

2. Владельцам **открытых и общедоступных государственных информационных ресурсов** осуществлять их включение в состав объектов международного информационного обмена только при **использовании сертифицированных средств защиты информации**, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации. А также осуществлять размещение технических средств, подключаемых к сети «Интернет», вне помещений, предназначенных для ведения закрытых переговоров.

Перечень сведений, доступ к которым не подлежит какому-либо ограничению (закон «Об информации...» ст. 8):

- нормативные правовые акты**, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информация о состоянии окружающей среды;**
- информация о деятельности государственных органов и органов местного самоуправления** (за исключением сведений, составляющих государственную или служебную тайну);
- информация, в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных для обеспечения граждан и организаций такой информацией;**
- информация, недопустимость ограничения доступа к которой установлена федеральными законами.**

Предоставляется бесплатно информация (ст. 8):

о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

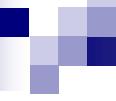
затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

иная информация, установленная законом.

Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях, установленных федеральными законами.

Контрольные вопросы

- 1. Виды режимов информации.**
- 2. Относится ли государственная тайна к конфиденциальной информации?**
- 3. Какая информация относится к персональным данным?**
- 4. Существует ли информация, которую запрещено относить к информации ограниченного доступа?**
- 5. В каких документах представлены нормы правового обеспечения защиты информации в компьютерных сетях?**
- 6. Назовите органы, осуществляющие контроль за соблюдением требований к защите информации.**
- 7. В каких документах указаны требования к безопасности компьютерных сетей в РФ?**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы по теме 2

- 1. Виды режимов информации.**
- 2. Относится ли государственная тайна к конфиденциальной информации?**
- 3. Какая информация относится к персональным данным?**
- 4. Существует ли информация, которую запрещено относить к информации ограниченного доступа?**
- 5. В каких документах представлены нормы правового обеспечения защиты информации в компьютерных сетях?**
- 6. Назовите органы, осуществляющие контроль за соблюдением требований к защите информации.**
- 7. В каких документах указаны требования к безопасности компьютерных сетей в РФ?**

3. Правовая защита государственной тайны

3.1. Сведения, составляющие государственную тайну

Система защиты государственных секретов основывается на

**Законе РФ «О государственной тайне» от 21.07.93г.
№5485-1 (ред. от 11 ноября 2003г. №153).**

Закон регулирует отношения, связанные с

отнесением сведений к государственной тайне (ГТ),

их рассекречиванием и

защитой в интересах безопасности РФ.

В законе даны следующие определения:

государственная тайна –

защищаемые государством сведения в области его

военной,

внешнеполитической,

экономической,

разведывательной,

контрразведывательной и

оперативно-розыскной деятельности,

распространение которых может нанести ущерб
безопасности РФ.

В законе даны следующие определения:

носители сведений, составляющих ГТ –

материальные объекты, в том числе физические поля, в которых сведения, составляющие ГТ, находят свое отображение в виде

**символов,
образов,
сигналов,
технических решений и
процессов.**

В законе даны следующие определения:

система защиты государственной тайны—совокупность

органов защиты ГТ,

используемых средств и

методов защиты сведений, составляющих ГТ, и их

носителей, а также

мероприятий, проводимых в этих целях.

Субъекты правоотношений:

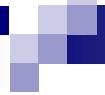
- органы государственного управления;**
- юридические лица**, независимо от их организационно-правовых форм деятельности и видов собственности;
- граждане и должностные лица**, которые взяли на себя обязательство либо обязаны по своему статусу выполнять требования законодательства о государственной тайне.

Перечень сведений, отнесенных к ГТ, утвержден

**Указом Президента РФ от 30.11.95г. №1203 (уточнен
Указом Президента РФ от 11.02.2006 № 90).**

**В частности, в сферах экономики, науки и техники к
государственной тайне относятся сведения:**

- о научно-исследовательских, опытно-конструкторских
и проектных работах, технологиях, имеющих важное оборонное
или экономическое значение;**
- о методах и средствах защиты секретной информации;**
- о государственных программах и мероприятиях в области
защиты государственной тайны.**



Правила, по которым определяется степень секретности сведений, представляющих ГТ утверждены

Постановлением Правительства РФ №870 от 04.09.95г.

Степень секретности сведений, составляющих ГТ,

должна соответствовать степени тяжести ущерба,

который может быть нанесен безопасности РФ

вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих ГТ, и соответствующие грифы секретности для носителей указанных сведений:

**"особой важности" (ОВ),
"совершенно секретно" (СС),
"секретно" (С).**

ОВ – если при разглашении наносится ущерб интересам РФ;

СС – если при разглашении наносится ущерб интересам отрасли или министерства;

С – если при разглашении наносится ущерб интересам предприятия.

При засекречивании сведений их носителям присваивается соответствующий гриф секретности.

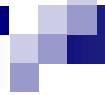
Существует также промежуточный гриф для документов,

которые не являются тайной предприятия, но

не предназначены для открытого использования:

ДСП – для служебного пользования.

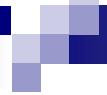
Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.



На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:

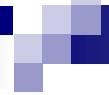
- о степени секретности содержащихся в носителе сведений

со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию.



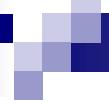
На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:

- об органе государственной власти,**
- о предприятии, об учреждении, организации, осуществлявших засекречивание носителя;**
- о регистрационном номере.**



На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:
-о дате или условии рассекречивания сведений.

При невозможности нанесения таких реквизитов на носитель сведений, составляющих ГТ, эти данные указываются в сопроводительной документации на этот носитель.



Порядок засекречивания сведений, составляющих ГТ, основан на трех принципах:

законности,

обоснованности и

своевременности.

Порядок засекречивания сведений, составляющих ГТ, основан на трех принципах:

Принцип законности

заключается в том, что засекречиванию не подлежат сведения, указанные в статье 7 закона о ГТ (которые раньше относились к ГТ).

Порядок засекречивания сведений, составляющих ГТ, основан на трех принципах:

Принцип обоснованности

заключается в установлении целесообразности

засекречивания сведений по экономическим

или иным критериям.

Порядок засекречивания сведений, составляющих ГТ, основан на трех принципах:

Принцип своевременности

заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

Не подлежат отнесению к государственной тайне и засекречиванию сведения (Статья 7):

-о чрезвычайных происшествиях и катастрофах;

-о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

Не подлежат отнесению к государственной тайне и засекречиванию сведения (Статья 7):

- о привилегиях и льготах гражданам, должностным лицам, предприятиям;**
- о фактах нарушения прав и свобод человека и гражданина;**

Не подлежат отнесению к государственной тайне и засекречиванию сведения (Статья 7):

-о размерах золотого запаса и государственных валютных резервах;

-о состоянии здоровья высших должностных лиц;

Не подлежат отнесению к государственной тайне и засекречиванию сведения (Статья 7):

-о фактах нарушения законности органами государственной власти и их должностными лицами.

Виновные в нарушении требований закона должностные лица могут быть привлечены к уголовной, административной или дисциплинарной ответственности.

Все граждане вправе обжаловать такие действия в суде.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью путем утверждения соответствующих перечней.

Обоснование необходимости отнесения сведений к ГТ в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Межведомственная комиссия по защите ГТ формирует, Перечень сведений, отнесенных к ГТ.

В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями.

Указанный Перечень утверждается Президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости.

Перечень должностных лиц, наделенных полномочиями по отнесению сведений к ГТ, утвержден распоряжением Президентом РФ от 30.05.97г. №226-рп «О перечне должностных лиц органов государственной власти, наделенных полномочиями по отнесению сведений к ГТ».

**Должностные лица, наделенные полномочиями по
отнесению сведений к государственной тайне, вправе
принимать решения о засекречивании информации,
находящейся у собственника информации, если эта
информация включает сведения, перечисленные в
Перечне сведений, отнесенных к ГТ.**

Засекречивание указанной информации
осуществляется по представлению собственников
информации или соответствующих органов
государственной власти.

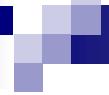
Материальный ущерб, наносимый собственнику информации в связи с ее засекречиванием, возмещается государством в соответствии с договором между органом государственной власти и ее собственником информации.

Не может быть ограничено право собственности на информацию иностранных юридических лиц и граждан, если она получена без нарушения законодательства РФ.

Постановлением Правительства РФ №170 от 20.02.95г установлен порядок рассекречивания и продления сроков засекречивания архивных документов.

Основания для рассекречивания сведений:

- взятие на себя РФ международных обязательств по открытому обмену сведениями, составляющими ГТ;**
- изменение обстоятельств, вследствие чего дальнейшая защита сведений является нецелесообразной.**

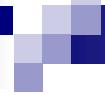


**Органы государственной власти обязаны каждые 5 лет
пересматривать содержание действующих перечней.**

**Срок засекречивания сведений, составляющих ГТ,
не должен превышать 30 лет.**

**В исключительных случаях этот срок может быть продлен по
заключению межведомственной комиссии по защите ГТ.**

**Носители сведений, составляющих ГТ, рассекречиваются не позднее
сроков, установленных при их засекречивании.**



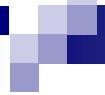
В статье 17 и 18 закона указан порядок передачи сведений, составляющих ГТ.

Передача сведений, составляющих ГТ, предприятиям, учреждениям, организациям или гражданам **осуществляется** с разрешения органа государственной власти только **при наличии**

у предприятия, лицензии на проведение работ с соответствующей степенью секретности, а

у граждан - соответствующего допуска.

Решение о передаче сведений, составляющих ГТ, другим государствам принимается Правительством РФ **при наличии** **экспертного заключения** межведомственной комиссии по защите ГТ о возможности передачи этих сведений.

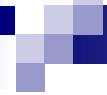


Режим защиты государственных секретов обеспечивается уполномоченными органами.

Эти органы организуют и обеспечивают защиту информации, содержащей ГТ в соответствии с функциями, возложенными на них законодательством РФ.

Органы защиты государственной тайны:

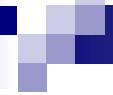
межведомственная комиссия по защите ГТ;
ФСБ,
МО,
СВР,
ФСТЭК.



Допуск должностных лиц и граждан к ГТ предусматривает:

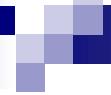
-принятие на себя обязательств перед государством по нераспространению сведений, составляющих ГТ;

-согласие на частичные, временные ограничения их прав в соответствии со статьей 24 настоящего Закона;



Допуск должностных лиц и граждан к ГТ предусматривает:

- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;**
- определение видов, размеров и порядка предоставления льгот, предусмотренных настоящим Законом;**



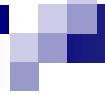
Допуск должностных лиц и граждан к ГТ предусматривает:

- ознакомление с нормами законодательства РФ о ГТ, предусматривающими ответственность за его нарушение;**

- принятие решения руководителем органа государственной власти или предприятия, о допуске лица к сведениям, составляющим ГТ.**

Для должностных лиц и граждан, допущенных к ГТ на постоянной основе, устанавливаются следующие льготы:

- процентные надбавки** к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;
- преимущественное право** при прочих равных условиях **на оставление на работе** при проведении организационных или штатных мероприятий.



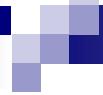
Постановлением Правительства РФ №573 от 18.09.2006г установлен размер ежемесячной процентной надбавки к должностному окладу.

За работу со сведениями имеющими степень секретности

"ОВ" надбавка составляет **50-75 %,**

"СС" надбавка составляет **30-50 %,**

"С" надбавка составляет **10-15 %.**



Устанавливаются **три формы допуска** к ГТ должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих ГТ:

Первая - к сведениям «ОВ»

Вторая - к сведениям «СС»

Третья - к сведениям «С»

Наличие у должностных лиц и граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Сроки, обстоятельства и порядок переоформления допуска граждан к ГТ устанавливаются нормативными документами Правительством РФ.

Порядок допуска должностных лиц и граждан к ГТ в условиях объявленного чрезвычайного положения может быть изменен Президентом РФ.

Особый порядок допуска к ГТ имеют.

Члены Совета Федерации,
депутаты Государственной Думы,
судьи на период исполнения ими своих полномочий,
адвокаты, участвующие в уголовном судопроизводстве по делам, связанным со сведениями, составляющими ГТ.

Эти лица допускаются к сведениям, составляющим ГТ, без проведения проверочных мероприятий, предусмотренных статьей 21 Закона.

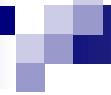
Особый порядок допуска к ГТ имеют.

Указанные лица предупреждаются о неразглашении ГТ, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем у них отбирается соответствующая расписка.

Сохранность ГТ в таких случаях гарантируется путем установления ответственности указанных лиц федеральным законом.

Должностное лицо или гражданин, допущенные к ГТ, могут быть временно **ограничены в следующих правах**:

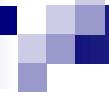
- права выезда за границу** на срок, оговоренный в трудовом договоре при оформлении допуска к ГТ;
- права на распространение сведений**, составляющих ГТ, и на использование открытых и изобретений, содержащих такие сведения;
- права на неприкосновенность частной жизни** при проведении проверочных мероприятий.



Допуск должностного лица или гражданина к РТ может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:

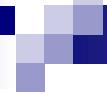
- расторжения с ним трудового договора в связи с проведением организационных и (или) штатных мероприятий**
- однократного нарушения им взятых на себя предусмотренных трудовым договором обязательств, связанных с защитой ГТ**

- возникновения обстоятельств, являющихся основанием для отказа должностному лицу или гражданину в допуске к ГТ
- прекращение допуска должностного лица или гражданина к ГТ является дополнительным основанием для расторжения с ним трудового договора, если такие условия предусмотрены в трудовом договоре.



Прекращение допуска к ГТ не освобождает должностное лицо или гражданина от взятых ими обязательств по неразглашению сведений, составляющих ГТ.

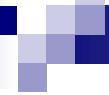
Решение администрации о прекращении допуска должностного лица или гражданина к ГТ и расторжении на основании этого с ним трудового договора может быть обжаловано в вышестоящую организацию или в суд.



Допуск предприятий и организаций к проведению работ, связанных

**с использованием сведений, составляющих ГТ,
с созданием средств защиты информации, а также
с осуществлением мероприятий и оказанием услуг по
защите ГТ,**

**осуществляется путем получения ими,
лицензий на проведение работ со сведениями
соответствующей степени секретности.**



**Лицензия на проведение указанных работ
выдается на основании результатов
специальной
экспертизы предприятия, учреждения и
организации и
государственной аттестации их
руководителей, ответственных за защиту
сведений, составляющих ГТ (ст. 27).**

Лицензия на проведение работ с использованием сведений, составляющих ГТ, выдается предприятию, учреждению, организации при выполнении ими следующих условий (ст. 27):

- выполнение требований**, утверждаемых Правительством РФ, по обеспечению защиты ГТ;
- наличие в их структуре подразделений по защите ГТ и** специально подготовленных сотрудников для работы по защите информации;
- наличие у них сертифицированных средств защиты** информации.



Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

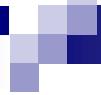
Организация сертификации средств защиты информации возлагается на
ФСБ, МО, ФСТЭК.

Сертификация осуществляется **на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ.**

3.2. Ответственность за разглашение ГТ

Ответственность за организацию защиты сведений, составляющих ГТ, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.

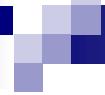
Должностные лица и граждане, виновные в нарушении законодательства РФ о ГТ, несут
уголовную,
административную,
гражданско-правовую или
дисциплинарную ответственность
в соответствии с действующим законодательством.



Уголовно-правовая ответственность за разглашение информации, содержащей ГТ, определяется **Уголовным кодексом РФ**
- ст. 275, 276, 283, 284.

Статья 275. Государственная измена

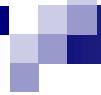
Государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности РФ,
совершенная гражданином РФ, -
наказывается лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей.



Уголовно-правовая ответственность за разглашение информации, содержащей ГТ, определяется **Уголовным кодексом РФ**
- ст. 275, 276, 283, 284.

Статья 276. Шпионаж

Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих ГТ, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности РФ, если эти деяния совершены иностранным гражданином или лицом без гражданства, - наказываются лишением свободы на срок от десяти до двадцати лет.

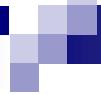


Уголовно-правовая ответственность за разглашение информации, содержащей ГТ, определяется **Уголовным кодексом РФ**
- ст. 275, 276, 283, 284.

Статья 283. Разглашение государственной тайны

Разглашение сведений, составляющих ГТ, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены - наказывается арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

То же деяние, с **тяжкими последствиями** - наказываются лишением свободы **от трех до семи лет** с лишением права занимать определенные должности на срок до трех лет.



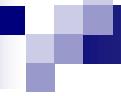
Уголовно-правовая ответственность за разглашение информации, содержащей ГТ, определяется **Уголовным кодексом РФ**
- ст. 275, 276, 283, 284.

Статья 284. Утрата документов, содержащих ГТ

Нарушение лицом, имеющим допуск к ГТ, установленных правил обращения с содержащими ГТ документами, если это повлекло по неосторожности их утрату и наступление тяжких последствий - наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет.

При установлении нарушений норм защиты информации используется понятие "**утраты документа**".

Утрата документов - это выход (в т.ч. и временный) документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могли стать достоянием посторонних лиц.



За обеспечением защиты ГТ установлен (ст. 30 и 32 закона)

ведомственный контроль осуществляют

**Органы государственной власти, наделенные в соответствии с
настоящим Законом полномочиями по распоряжению сведениями,
составляющими ГТ, обязаны контролировать эффективность
защиты этих сведений во всех подчиненных и подведомственных
их органах государственной власти,
на предприятиях,
в учреждениях и
организациях,
осуществляющих работу с ними.**

межведомственный контроль

осуществляют:

- федеральный орган исполнительной власти,
уполномоченный в области обеспечения
безопасности,**
- федеральный орган исполнительной власти,
уполномоченный в области обороны,**
- федеральный орган исполнительной власти,
уполномоченный в области внешней разведки,**
- федеральный орган исполнительной власти,
уполномоченный в области противодействия
техническим разведкам и технической защиты
информации, и их территориальные органы, на
которые эта функция возложена законодательством
РФ.**

За обеспечением защиты ГТ установлен

**Контроль за обеспечением защиты ГТ
осуществляют**

Президент и Правительство РФ.

**Надзор за соблюдением законодательства
осуществляют**

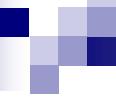
**Генеральный прокурор РФ и подчиненные ему
прокуроры.**

Меры предупреждения нарушений режима секретности:

- 1.Правильный профотбор кадров.**
- 2.Ограничение доступа к секретам.** /Каждый сотрудник должен иметь доступ только к той информации, которая ему необходима в процессе выполнения прямых служебных обязанностей/.
- 3.Проведение воспитательной работы.** /Стимулирование за поддержание режима секретности и строгие наказания за нарушения/.
- 4.Подписание соглашений с работниками о неразглашении.**
- 5.Политика «чистых столов».**
- 6.Создание службы безопасности фирмы.**
- 7.Использование технических средств защиты.**
- 8.Применение сертифицированных программных и аппаратных средств ЗИ в информационных системах.**

Контрольные вопросы

- 1. На каком законе РФ основывается система защиты государственных секретов?**
- 2. Какую информацию относят к сведениям, составляющим государственную тайну?**
- 3. Назовите степени секретности, установленные для сведений, составляющих государственную тайну?**
- 4. На каких принципах основан порядок засекречивания сведений, составляющих государственную тайну?**
- 5. Кем установлен порядок рассекречивания и продления сроков засекречивания архивных документов?**
- 6. Ответственность за разглашение информации, содержащей государственную тайну.**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы по теме 3

- 1. Какую информацию относят к сведениям, составляющим государственную тайну?**
- 2. Условия допуска физических и юридических лиц к ГТ.**
- 3. Ограничения прав работников при допуске их к ГТ.**
- 4. Какие льготы имеют работники допущенные к ГТ?**
- 5. Сроки засекречивания и пересмотра грифов секретности.**
- 6. Основания выдачи лицензии предприятиям на проведение работ с использованием государственных секретов.**
- 7. Ответственность за разглашение информации, содержащей государственную тайну.**

4. Правовая защита коммерческой тайны

4.1. Сведения, составляющие коммерческую тайну

В условиях жесткой конкуренции фирмы сбор информации о рынке, о партнерах и другой полезной информации как правило носит разведывательный характер.

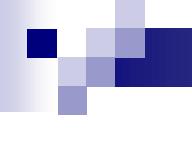
Главным предметом разведки является КОММЕРЧЕСКАЯ ТАЙНА.

Принято различать:

конкурентную разведку ("деловая разведка", "бизнес-разведка") и

промышленный шпионаж.

Отличие заключается в соблюдении закона в первом случае и нарушениях уголовного, авторского или любого другого права - во втором.



Конкурентная разведка – это сбор и обработка информации законными способами.

На данный момент в нашей стране под конкурентной разведкой подразумеваются четыре вида сбора информации:

- 1. Сбор данных о партнерах и клиентах для предотвращения мошенничества с их стороны.**

- 2. Информация о потенциальных партнерах и сотрудниках.** Обычно этим занимаются отделы безопасности компаний или частные детективные агентства.

- 3. Выполнение услуг охраны и сыска, предусмотренных Законом "О частной детективной и охранной деятельности".**
- 4. Сбор информации маркетингового характера.**

Именно это направление понимается на Западе под конкурентной разведкой.

Виды конкурентной разведки (сбор информации маркетингового характера):

наблюдение;

отчеты торговых работников;

поиск информации в открытых БД;

анализ годовых отчетов предприятий;

обратный инжиниринг.

В настоящее время широко используется

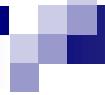
конкурентная разведка через Интернет.

Выделяют три режима такой разведки:

оперативный (сбор и предоставление информации за 10 мин.)

ситуационный центр (подготовка информации руководству с выводом на экран за 3-4 часа) и

оперативные исследования (проведение исследований и подготовка отчета за 1-2 дня).



Промышленный шпионаж - незаконный сбор сведений, составляющих коммерческую тайну, незаконное использование секретной информации лицом или предприятием, не уполномоченным на то ее владельцем.

В мире существуют тайные биржи, где продают промышленные секреты: например,

в Японии - по электронике и пластмассам,

в Италии - по фармацевтике,

на Украине на черном информационном рынке.

/Скрипник, Ф. Экономический шпионаж и разведка // Финансовый директор ISSN 1680-1148. – 2003. – №2. – С. 17–22./

Понятие “коммерческая тайна” в нашем законодательстве впервые появилось в 1990 году в тексте Закона "О предприятиях и предпринимательской деятельности".

Затем в Законе РФ "Об информации, информатизации и защите информации", от 25.01.95г.,

в Гражданском кодексе РФ, в 1994г. ч.1. и

в Законе РФ "О коммерческой тайне", от 29.07.2004г.

К КТ относят следующие три группы сведений:

1. Деловая информация (о сферах деятельности):

-финансовые сведения;

-данные о себестоимости продукции и услуг;

-деловые планы и планы производства и развития;

-информация о маркетинге;

-соглашения, предложения, контракты;

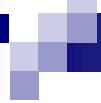
-организационные схемы.



К КТ относят следующие три группы сведений:

2. Техническая информация:

- научно-исследовательские проекты;
- конструкторская документация на продукцию;
- заявки на патенты;
- дизайн, передовые технологии и оборудование;
- программное обеспечение ЭВМ и информационный процесс;
- химические формулы.



К КТ относят следующие три группы сведений:

3. Информация о клиентах и конкурентах

На каждого клиента фирмы накапливается информация, где отражаются его привычки, характерные черты поведения, интересы в личной жизни, о представляемых ему фирмой привилегиях и т.п.

Аналогичные базы данных составляют и на своих конкурентов.

Таким образом, формируются

«профиль клиента» и

«профиль конкурента».

Существует три основных направления сбора информации, представляющей коммерческий интерес.

1. Информация о рынке (издается и публикуется):

- цены, условия договоров, скидки;
- объем, тенденции и прогнозы сбыта продуктов;
- доля на рынке и тенденция ее изменения;
- рыночная политика и планы;
- отношения с потребителями и репутация;
- численность и расстановка торговых агентов;
- каналы, политика и методы сбыта;
- постановка рекламы.

2. Информация о производстве продукции (закупки, наблюдение, опрос):

- оценка качества и эффективности;
- номенклатура изделий;
- технология и оборудование;
- уровень издержек;
- производственные мощности;
- способ упаковки;
- доставка;
- размещение и размер производственных подразделений и складов;
- результаты НИОКР.

3. Информация об организационных особенностях и планах развития:

- выявление лиц, принимающих ключевые решения (ЛПР);
- программы развития фирмы;
- главные проблемы и возможности их решения;
- программы проведения научно-исследовательских работ.

Сведения о деятельности фирмы и ее руководителях собирают в различных экономических газетах и журналах, справочниках, выписывают у биржевиков, покупают у частных детективов, а также с помощью конкурентной разведки через Интернет.

В настоящее время существуют аналитические структуры, учрежденные крупнейшими финансово-промышленными группами, задачи которых заключаются в сборе данных на все фирмы, зарегистрированные в данном регионе: их оборот, уставной капитал, принадлежащая им недвижимость, точность в расчетах, отношения с налоговыми, административными, судебными инстанциями.

Подобным предприятием в России является фирма “РУСС-ИГК” /Москва/.

За умеренную плату она представляет своим клиентам необходимую информацию.

4.2. Защита коммерческой тайны

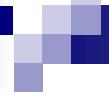
Чем отличается коммерческая тайна от государственной?

- 1. Сведения, составляющие ГТ, установлены соответствующим перечнем, а КТ этим перечнем не определена, и определяется руководителем предприятия.**

- 2. ГТ охраняется силой государства в лице соответствующих органов, а коммерческая информация – службой безопасности предприятия.**

Основное отличие связано с тем чьи интересы страдают в случае ее разглашения в одном случае – государства, в другом – коммерческой фирмы. Соответственно и методы используемые в одном случае могут использоваться и в другом.

По аналогии с ГТ коммерческая информация может быть ранжирована по степени ее важности для предприятия с тем, чтобы регулировать ее распространение среди работающих на предприятии, указывать пользователей этой информации, уровень ее защиты и т.д.



Для обозначения степени важности коммерческой информации для предприятия можно предложить систему обозначения степени ее секретности:

Коммерческая тайна – строго конфиденциально (КТ-СК)

Коммерческая тайна – конфиденциально (КТ-К)

Коммерческая тайна (КТ)

**Промежуточный гриф рекомендуется использовать
ДВИ – для внутреннего использования.**

Закон "О коммерческой тайне" 29 июля 2004 года N 98

регулирует отношения, связанные с отнесением информации к КТ, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции, а также определяет сведения, которые не могут составлять КТ.

КТ - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (ст. 3)

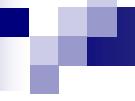
КТ - это научно-техническая, технологическая, производственная, финансово-экономическая информация в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

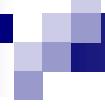
Режим коммерческой тайны - правовые, организационные, технические и иные меры по охране ее конфиденциальности.



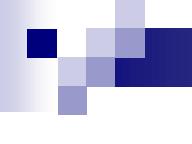
Не могут составлять КТ (ст. 5) сведения:

- 1) содержащие в **учредительных документах** юридического лица, и индивидуальных предпринимателях;
- 2) дающие **право на осуществление предпринимательской деятельности**;
- 3) о **составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов**;

- 
- 4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической обстановке и других факторах;**
 - 5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;**



- 6) о **нарушениях законодательства РФ** и фактах привлечения к ответственности за совершение этих нарушений;
- 7) об **условиях конкурсов** или аукционов по приватизации **объектов государственной или муниципальной собственности**;
- 8) о размерах и структуре доходов **некоммерческих организаций**, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

- 
- 9) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;**
 - 10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;**
 - 11) сведения, недопустимость ограничения доступа к которым установлена иными федеральными законами.**

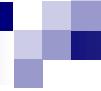
Обладатель информации, составляющей КТ, по требованию органа государственной власти предоставляет ее на безвозмездной основе (ст. 6).

Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей КТ, и срок предоставления этой информации.

Режим коммерческой тайны является обязательным условием охраны конфиденциальности информации

Законом о КТ установлены требования, предъявляемые к режиму коммерческой тайны

Режим КТ считается установленным, после принятия обладателем информации следующих мер (ст. 10 и 11):



- 1) определение перечня информации, составляющей КТ;**
- 2) ограничение доступа к информации, составляющей КТ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;**
- 3) учет лиц, получивших доступ к информации, составляющей КТ, и (или) лиц, которым такая информация была предоставлена или передана;**

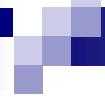
- 4) регулирование отношений по использованию информации, составляющей КТ, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;**
- 5) нанесение на документы, содержащие КТ, грифа "Коммерческая тайна" и обладателя этой информации**
- для юридических лиц** - полное наименование и место нахождения,
- для индивидуальных предпринимателей** — фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства.



- 6) ознакомить **под расписку** работника с перечнем информации, составляющей КТ;
- 7) **создать** работнику **необходимые условия** для соблюдения им установленного работодателем режима КТ;
- 8) ознакомить **под расписку** работника с **установленным** работодателем **режимом КТ** и с мерами ответственности за его нарушение.

Доступ работника к информации, составляющей КТ, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

В случае нарушения конфиденциальности информации должностными лицами органов государственной власти эти лица несут ответственность в соответствии с законодательством РФ (ст. 13).



Ответственность за нарушение настоящего закона (ст. 14).

Нарушение закона влечет за собой

дисциплинарную,

гражданско-правовую,

административную или

уголовную ответственность

в соответствии с законодательством РФ.

**Органы государственной власти, несут
гражданско-правовую ответственность за
разглашение или незаконное использование
КТ их должностными лицами,
которым она стала известна в связи с выполнением
ими должностных обязанностей (ст. 14).**

Лицо, которое использовало информацию, составляющую КТ, и не имело достаточных оснований считать использование данной информации незаконным, (получило доступ к ней в результате случайности или ошибки), не может быть привлечено к ответственности (ст. 14).

Невыполнение обладателем информации, составляющей КТ, законных требований органов государственной власти о предоставлении им информации, составляющей КТ, влечет за собой ответственность в соответствии с законодательством РФ (ст. 15).

Ответственность за разглашение КТ, дана в УК РФ ст. 183 - Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом - наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до двух лет.

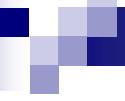
2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, -

наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до 3-х лет.

- 3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до пяти лет.**
- 4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, наказываются лишением свободы на срок до десяти лет.**

Контрольные вопросы

- 1. Какую информацию относят к сведениям, составляющим КТ?**
- 2. Виды конкурентной разведки.**
- 3. Отличие конкурентной разведки от промышленного шпионажа.**
- 4. Какой закон регулирует отношения по защите КТ?**
- 5. Сведения, которые не могут составлять КТ.**
- 6. Что значит ввести режим КТ на предприятии?**
- 7. Ответственность за разглашение информации, содержащей КТ.**
- 8. Какие грифы конфиденциальности может использовать предприятие для обозначения степени важности коммерческой информации?**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы по теме 4 (4.1. 4.2.)

- 1. Какую информацию относят к сведениям, составляющим КТ?**
- 2. Виды конкурентной разведки.**
- 3. Отличие конкурентной разведки от промышленного шпионажа.**
- 4. Кокой закон регулирует отношения по защите КТ?**
- 5. Сведения, которые не могут составлять КТ.**
- 6. Что значит ввести режим КТ на предприятии?**
- 7. Ответственность за разглашение информации, содержащей КТ.**

4. Правовая защита коммерческой тайны

4.3. Правовое регулирование отношений по защите КТ на предприятии

В соответствии с установленными законом о КТ на предприятии используются правовые нормы внутрифирменных документов для регулирования правовых отношений по защите КТ.

Такими документами являются:

- 1.Устав предприятия;**
- 2.Коллективный договор предприятия;**
- 3.Трудовые и гражданско-правовые договоры;**
- 4.Правила внутреннего трудового распорядка рабочих и служащих предприятия;**
- 5.Должностные обязанности руководителей, специалистов, рабочих и служащих предприятия.**
и другие документы.

Для создания правовых основ защиты информации на коммерческом предприятии необходимо:

1. Ввести в Устав предприятия в раздел “Права и обязанности предприятия”:

“Предприятие имеет право определять состав, объем и порядок защиты сведений, составляющих КТ, требовать от сотрудников предприятия обеспечения ее сохранности”.

“Предприятие обязано обеспечить сохранность КТ”.

Внесение этих требований дает право администрации предприятия:

- создавать организационные структуры по защите КТ;**
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих КТ, и механизмы ее защиты;**
- включать требования по защите КТ в договора по всем видам хозяйственной деятельности;**
- требовать защиту интересов предприятия перед государственными и судебными органами.**

2. Разработать “Перечень сведений, составляющих КТ предприятия” и довести его под роспись до всех сотрудников.

3. Дополнить “Коллективный договор” следующими требованиями:

В раздел “Предмет договора”

Администрация предприятия обязуется обеспечить разработку и осуществление мероприятий по введению режима и защите КТ.

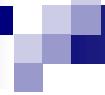
Трудовой коллектив принимает на себя обязательство по соблюдению установленных на предприятии требований по защите КТ.

В раздел “Кадры”

Администрация обязуется привлекать нарушителей требований по защите КТ к административной и уголовной ответственности в соответствии с действующим законодательством.

4. Дополнить правила внутреннего распорядка дня работников требованиями о неразглашении КТ.

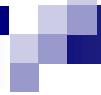
При поступлении рабочего или служащего на работу, переходе его на другую работу а также при увольнении, администрация обязана проинструктировать работника по правилам сохранения КТ с оформлением письменного обязательства о ее неразглашении.



5. Ввести в текст трудового договора требования по защите КТ.

Тогда независимо от формы заключения договора (устная или письменная) подпись работника на приказе о приеме на работу подтверждает его согласие с условиями договора.

Если договор заключается в устной форме, то действует требование по защите КТ, вытекающее из правил внутреннего трудового распорядка.



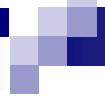
6. В должностные обязанности руководителей, специалистов, рабочих и служащих записать, что:

-сотрудники должны знать относящиеся к их деятельности сведения, являющиеся КТ, выполнять лично требования по ее защите и принимать меры по предупреждению нарушений установленных норм сохранности КТ.

Включение этих требований дает право администрации предприятия применять к нарушителям меры дисциплинарного воздействия в соответствии с Трудовым кодексом РФ.

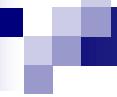
Руководителю предприятия, при создании системы безопасности на своей фирме, необходимо определить следующее:

- какая информация нуждается в защите;**
- кого она может заинтересовать;**
- каков “срок жизни” этих секретов;**
- во что обойдется их защита.**



В рамках режима КТ на предприятии вводятся система закрытого делопроизводства, которая включает:

- 1. Создание отдела защищенного делопроизводства (ОЗД).**
- 2. Проведение документирования:**
 - определение перечня документов, содержащих секреты предприятия;
 - контроль за содержанием документов и степени секретности;
 - контроль за размножением и рассылкой документов;
 - учет документов с грифом “КТ” (производится отдельно от несекретных документов и документов ДВИ) включает:
 - регистрация каждого вх. и исх. документа;
 - инвентарный учет;
 - номенклатуру дел, журналов и карточек;
 - контроль за местоположением документов.



Корреспонденция с грифом “КТ” поступает в ОЗД, где она проверяется на наличие недостачи и регистрируется на карточках или в журнале.

Листы журналов нумеруются, прошиваются и опечатываются.

На первом листе зарегистрированного входящего документа с грифом “КТ” ставится штамп

Наименование предприятия		
Входящий № и дата	Количество листов	
	основных	приложений

Исходящие документы с грифом “КТ” печатаются в машбюро ОЗД или с учтенных носителей с помощью средств ВТ.

На последнем листе каждого экземпляра проставляется количество отпечатанных экземпляров, фамилия исполнителя, машинистки и дата.

Отпечатанный документ регистрируется в журнале.

Все черновики выполняются на предварительно учтенных в ОЗД листах, сдаются после окончания работы и уничтожаются в ОЗД.

Отправка документов с грифом “КТ” производится заказными письмами или бандеролями.

При этом рекомендуется использовать двойной конверт, причем, на внешнем пишется адрес, а на внутреннем ставится гриф.

Проверка наличия документов проводится

ежеквартально- для документов, находящихся на исполнении

ежегодно- для всех зарегистрированных документов.

Режимные документы, находящихся у сотрудников на исполнении, хранятся на предприятии в опечатанных папках или чемоданах .

3. Организацию документооборота:

- установление разрешительной системы доступа исполнителей к документам;
- установление грифа секретности (степени секретности);
- установление порядка приема передачи документов между сотрудниками;
- контроль за порядком работы с документами;
- установление порядок хранение и уничтожение документов;
- установление порядка обращения с документами.

Порядок хранение и уничтожение документов включает:

- выделение специально оборудованных помещений;
- установление порядка доступа к делам;
- контроль за своевременностью и правильностью формирования дел;
- установление порядка подготовки документов для уничтожения;
- обеспечение необходимых условий уничтожения;
- контроль за правильностью и своевременностью уничтожения документов.

Порядок обращения с документами

1. Выдача документов с грифом КТ сотрудникам производится по разрешению руководителя предприятия на основании служебной записки от начальника подразделения исполнителя.
2. Передача документов с грифом “КТ” между сотрудниками осуществляется под расписку и в пределах круга лиц, допущенных к данному документу.
3. После окончания рабочего дня помещения ОЗД передаются под охрану.
4. Разрешение на уничтожение документа дает руководитель подразделения, к деятельности которого относится документ, путем записи в журнал учета «Уничтожить», подпись, дата.
5. Уничтожение документов производится путем их сожжения или измельчения.

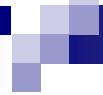
4.4. Защита коммерческой информации в договорной документации

Правовая защита коммерческих секретов, основывается на использовании таких внутрифирменных нормативных документов как **трудовой договор** (контракт) и **должностные инструкции**.

Содержанием трудового договора являются взаимные права и обязанности и установлена ответственность при исполнении должностных инструкций.

В трудовом договоре принято различать **основные** (законодательно определенные) и **дополнительные** (факультативные) условия.

Вопросы защиты информации закрепляются в трудовом договоре в виде **дополнительных условий**.



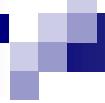
В обязанности работника включают условие о неразглашении служебной (коммерческой) тайны, к которой он будет допущен в силу его должностных обязанностей.

Кроме трудового договора данное условие может быть также включено и в другие виды договоров:

- договор поручительства;**
- договор коммерческого представительства;**
- агентский договор;**
- договор поручения или доверенности;**
- договор о рекламных услугах;**
- другие информационные услуги.**

В этих документах включаются следующие обязательства:

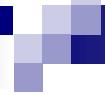
- не разглашать КТ организации третьим лицам или публично без согласия администрации;
- сохранять КТ тех организаций, с которыми имеются деловые связи;
- выполнять требования приказов и инструкций по защите КТ предприятия;
- не использовать секретные сведения организации, занимаясь другой деятельностью (ущерб от конкурентного действия);
- незамедлительно извещать СБ о попытках посторонних лиц получить закрытую информацию;
- незамедлительно извещать об утрате носителей секретной информации и другие факты нарушения режима ее защиты;
- при увольнении все носители КТ с которыми работал сотрудник передаются соответствующему должностному лицу;
- предупреждение работника о наступлении гражданской, административной или уголовной ответственности в случае нарушения взятых обязательств.



Обязанности по сохранению КТ возлагаются и на руководителя организации.

Для этого в контракт, заключаемый с руководителем вводятся соответствующие положения:

- обязательство руководителя хранить КТ и не использовать ее в ущерб организации;**
- о персональной ответственности за создание необходимых условий для сохранности КТ;**
- об ответственности руководителя за нарушения режима защиты КТ и возможных последствиях.**



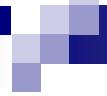
Защита прав обладателя коммерческих секретов осуществляется способами, предусмотренными также ГК РФ и другими законами.

Среди них можно выделить следующие:

пресечение действий, нарушающих право или создающих угрозу его нарушения;

возмещение убытков, в том числе и упущенной выгоды (ГК РФ ст. 12, 15).

Убыток - это выраженный в денежной форме ущерб, который состоит из затрат, связанных с созданием этих документов (например, стоимость бумаги) и упущенной выгоды, т.е. из доходов, которые могло бы получить предприятие в случае сохранения тайны.



4.5. Правовая защита от компьютерных преступлений

Средства автоматизированной обработки информации с использованием ЭВМ имеют ряд особенностей, дающих широкие возможности для злоумышленных действий.

Потери от КП во всем мире достигают в миллиарды долларов в год.
Особенно страдают кредитно-финансовые учреждения.

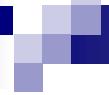
Кроме этих действий значительные потери возникают в результате распространения вредоносных программ - компьютерных вирусов, появившиеся с 1987г.

Особенностью компьютерных преступлений является то, что их жертвы не всегда обращаются за защитой в правоохранительные органы (по коммерческим соображениям).

Можно выделить следующие
виды угроз информации в АС.

1.Перехват информации:

- по электромагнитному излучению** (излучения ЭЛТ можно принимать на расстояниях до 1000 м.);
- по виброакустическому каналу** (таблетки, клопы, жучки, через несущие конструкции и проемы здания, стетоскоп);
- видеоперехват** (бинокль, фото- и видеокамеры);
- использование отходов информационного процесса** (физические - дискеты, пленки и “мусор” в памяти компьютера).



2. Несанкционированный доступ (НСД) к информации:

-физическое проникновение;

-установка шлейфов;

-подключение к линии связи законного пользователя;

-подбор кода доступа в т.ч. с помощью
программ-“взломщиков”, вручную с помощью
“интеллектуального” перебора - вскрывается 42%
паролей из 8 символов.

3. Манипуляция данными и управляющими командами:

- умышленное изменение данных;
- изменение логических связей в электронных цепях и топологии микросхем.

4. Компьютерные вирусы.

“Троянский конь” - программа выдает себя за известную

“Троянская матрешка” - программа создает “троянского коня” и самоуничтожается.

“Троянский червь” - реализуется саморазмножения.

“Логическая бомба” - программа активируется при стечении определенных обстоятельств (включает алгоритм “троянского коня”) или в определенный момент времени “временная бомба”.

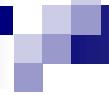
“Воздушный змей” переброска средств с одного счета на другой и обратно с постепенным увеличением сумм.

5.Использование специальных программных средств:

**-“моделирование” процессов и способов преступления
путем создания игровой программы
защита-преодоление.**

6.Комплексные методы.

Использование двух и более способов и их комбинации.



Эффективная борьба с КП в РФ ведется с 1997г. после принятия УК РФ, в котором помещена глава 28 «Преступления в сфере компьютерной безопасности».

Составы компьютерных преступлений даны в следующих статьях:

- «Неправомерный доступ к компьютерной информации» (ст. 272);
- «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273);
- «Нарушение правил эксплуатации ЭВМ» (ст. 274).

Статья 272. Неправомерный доступ к компьютерной информации

- 1. Неправомерный доступ к компьютерной информации**, то есть информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, или их сети, - **наказывается штрафом в размере до двухсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, **либо лишением свободы на срок до двух лет.**
- 2. То же деяние, совершенное организованной группой** либо лицом с использованием своего служебного положения, имеющим доступ к ЭВМ,- **наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, **либо лишением свободы на срок до пяти лет.**

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

- 1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами -**
наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.
- 2. Те же деяния, повлекшие по неосторожности тяжкие последствия, -**
наказываются лишением свободы на срок от трех до семи лет.

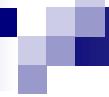


Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.



Целям защиты информации, обрабатываемой в АС
служит принятый 2002 г.

**Закон РФ «Об электронной цифровой подписи» (в ред
ФЗ "Об электронной подписи" от 6 апреля 2011 г. N 63-ФЗ)**

**ЭЦП – реквизит документа, полученный в результате
криптографического преобразования информации
с использованием закрытого ключа электронной цифровой
подписи и позволяющий идентифицировать владельца
сертификата ключа подписи, а также установить отсутствие
искажения информации в электронном документе (ст. 3)
признается равнозначной собственноручной подписи
лица на бумажном носителе, заверенном печатью (ст. 19).**

Контрольные вопросы

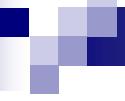
- 1. Какие внутрифирменные документы, использует предприятие для регулирования правовых отношений по защите конфиденциальной информации?**

- 2. В какие виды договоров может быть также включено условие о неразглашении служебной (коммерческой) тайны?**

- 3. Какими способами осуществляется защита прав обладателя коммерческой тайны?**

- 4. Назовите виды угроз информации в автоматизированных системах?**

- 5. Где указаны нормы ответственности за компьютерные преступления?**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 4.2

- 1. Какие внутрифирменные документы, использует предприятие для регулирования правовых отношений по защите конфиденциальной информации?**
- 2. В какие виды договоров может быть также включено условие о неразглашении коммерческой тайны?**
- 3. Какими способами осуществляется защита прав обладателя коммерческой тайны?**
- 4. Назовите виды угроз информации в автоматизированных системах?**
- 5. Где указаны нормы ответственности за компьютерные преступления?**
- 6. На каких законах основана правовая защита электронных документов?**

5. Правовые основы использования организационных и технических методов защиты информации

5.1. Правовые основы деятельности службы безопасности

Служба безопасности (СБ) фирмы это самостоятельное структурное подразделение, которое решает задачи обеспечения защиты жизненно важных интересов фирмы в условиях коммерческого риска и конкурентной борьбы.

Деятельность СБ должна быть основана на государственных и внутрифирменных нормативных документах.

Законы РФ:

«О частной детективной и охранной деятельности» от 11.3.1992 №2487-1, ред. от 10.01.2003 №15-ФЗ,
«О безопасности» от 5.3.1992 №2446-1,
«Об оружии» от 13.12.1996 №150-ФЗ,
«Об информации...» от 27.13.2006 № 149-ФЗ,
«О ведомственной охране» от 14.4.1999 №77-ФЗ,
ГК РФ и Трудовой Кодекс.

Постановления Правительства РФ:

«Вопросы частной детективной и охранной деятельности» от 14.8.1992 №587,
«Об организации ведомственной охраны» от 12.7.2000 №514.

Внутренние документы:

- Устав фирмы, трудовые договоры, правила внутреннего трудового распорядка, должностные обязанности руководителей, специалистов, рабочих и служащих, положение о СБ;**
- инструкция по организации режима и охраны;**
- инструкция по защите КТ;**
- перечень сведений, составляющих КТ;**
- инструкция по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;**
- инструкция по хранению документов, содержащих КТ в архиве;**
- инструкция по инженерно - технической защите информации;**
- инструкция о порядке работы с иностранными представителями.**

Основным документом, регулирующим вопросы создания и деятельности СБ, является

Закон РФ «О частной детективной и охранной деятельности», №2487-1 от 11.03.92г. (ред. от 07.02.2011 N 4-ФЗ)

Основные положения:

- Частная детективная и охранная деятельность **осуществляется физическими и юридическими лицами**, имеющими специальное разрешение (**лицензию**) (ст.1,4), которая выдается **органом внутренних дел** (лица, занимающиеся частной детективной деятельностью, не вправе осуществлять оперативно – розыскные действия).
- **Предприятия**, независимо от организационно-правовых форм, **вправе учреждать** обособленные подразделения (**службы безопасности**) для осуществления охранно-сыскной деятельности в интересах собственной безопасности учредителя (ст.14).

В целях сыска

разрешается предоставление следующих
7 видов услуг (ст. 3):

- **сбор сведений** по гражданским делам;
- **изучение рынка**, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;
- **установление фактов** недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;

- **выяснение биографических и других данных** об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов;
- **поиск без вести пропавших** граждан;
- **поиск утраченного имущества;**
- **сбор сведений по уголовным делам** на договорной основе с участниками процесса. В течение суток с момента заключения контракта с клиентом на сбор таких сведений частный детектив обязан письменно уведомить об этом следователя, прокурора или суд, в чьем производстве находится уголовное дело.

В целях охраны

разрешается предоставление следующих **5 видов услуг:**

- **защита жизни и здоровья граждан;**
- **охрана имущества собственников;**
- **проектирование, монтаж и эксплуатационное обслуживание средств охранно - пожарной сигнализации;**
- **консультирование клиентов по вопросам защиты от противоправных посягательств;**
- **обеспечение порядка в местах проведения массовых мероприятий.**

При осуществлении частной сыскной деятельности допускается (ст. 5):

- **использование видео- и аудиозаписи, кино- и фотосъемки,**
- **технических и иных средств, не причиняющих вреда жизни и здоровью граждан и окружающей среде,**
- **средств оперативной радио- и телефонной связи,**
- **устный опрос граждан и должностных лиц (с их согласия), наведение справок, изучение предметов и документов (с письменного согласия их владельцев), внешний осмотр строений, помещений и других объектов.**

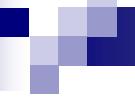
Частным детективам запрещается (ст. 7):

- **выдавать себя за сотрудников правоохранительных органов;**
- **осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц;**
- **проведение сыскных действий**, нарушающих тайну переписки, телефонных переговоров и телеграфных сообщений либо связанных с нарушением гарантий неприкосновенности личности или жилища;

- скрывать от правоохранительных органов ставшие им известными факты готовящихся, совершаемых или совершенных преступлений;
- разглашать сведения, касающиеся вопросов обеспечения защиты жизни и здоровья граждан и (или) охраны имущества заказчика;
- получать и использовать информацию органов, осуществляющих оперативно-розыскную деятельность;
- использовать методы сыска (ст. 12).

Лицензия не выдается (ст. 6):

- 1) гражданам, не достигшим двадцати одного года;**
- 2) гражданам, состоящим на учете в органах здравоохранения по поводу психического заболевания, алкоголизма или наркомании;**
- 3) гражданам, имеющим судимость за совершение умышленного преступления;**
- 4) гражданам, которым предъявлено обвинение в совершении преступления (до разрешения вопроса об их виновности в установленном законом порядке);**

- 
- 5) гражданам, уволенным с государственной службы, из судебных, прокурорских и иных правоохранительных органов по компрометирующим их основаниям;**
 - 6) бывшим работникам правоохранительных органов, осуществлявшим контроль за частной детективной и охранной деятельностью, если со дня их увольнения не прошел год;**
 - 7) гражданам, не представившим документы, перечисленные в части второй настоящей статьи.**

Продление срока действия удостоверения частного охранника осуществляется только после повышения квалификации в образовательных учреждениях (ст. 11).

Частная охранная организация может быть создана только в форме общества с ограниченной ответственностью и **не может осуществлять иную деятельность, кроме охранной** (ст. 15).

В статью 15.

Руководитель частной охранной организации должен иметь высшее профессиональное образование и пройти повышение квалификации для руководителей частных охранных организаций.

Обязательное требование - наличие у руководителя частной охранной организации удостоверения частного охранника (ст. 15).

В ходе осуществления **частной детективной деятельности** разрешается применять –

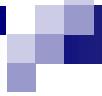
➤ **специальные средства,**

а при осуществлении **частной охраной деятельности** –

➤ **специальные средства и огнестрельное оружие** только в случаях и в порядке, предусмотренных настоящим Законом.

Охранник при применении специальных средств или огнестрельного оружия обязан:

- **предупредить** о намерении их использовать;
- **стремиться, чтобы любой ущерб, причиненный при устраниении опасности, был минимальным;**
- **немедленно уведомить прокурора** о всех случаях смерти или причинения телесных повреждений.



Перечень видов специальных средств, используемых группой охраны СБ в соответствии с данным законом и Постановлением Правительства от 14.8.1992 N 587:

- жилет защитный;
- шлем защитный;
- спецсредство «Черемуха» и его аналоги ТУ 6-02-832-76;
- газовый пистолет ТУ БВ-Г.000;
- наручники ТУ 87.2.026-88;
- палка резиновая (пластиковая).

Виды вооружения охранников, (порядок приобретения, учета, хранения и ношения оружия регламентируются Правительством РФ):

- **9мм пистолет ПМ ТУ 9375-88;**
- **ружье охотничье гладкоствольное ТУ 3-3.1421-83;**
- **боеприпасы к оружию ТУ А9003-80.**

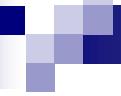
Частные детективы и охранники обязаны проходить периодическую проверку на пригодность к действиям в условиях, связанных с применением специальных средств и огнестрельного оружия, определяемой МВД.

На частную детективную и охранную деятельность распространяются правила применения специальных средств, установленные Правительством РФ для органов внутренних дел.

Частные детекти́вы и охра́нники имею́т право применять (ст. 18):

1) специальны́е средства в следую́щих случаях:

- **для отражения нападения;**
- **для пресечения преступления, когда правонарушитель оказывает физическое сопротивление.**



2) огнестрельное оружие

- для отражения нападения;
- для предупреждения (выстрелом в воздух).

Контроль и надзор за частной детективной и охранной деятельностью (ст. 20).

Контроль за частной детективной и охранной деятельностью осуществляют Министерство внутренних дел.

Надзор за исполнением настоящего Закона осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры.

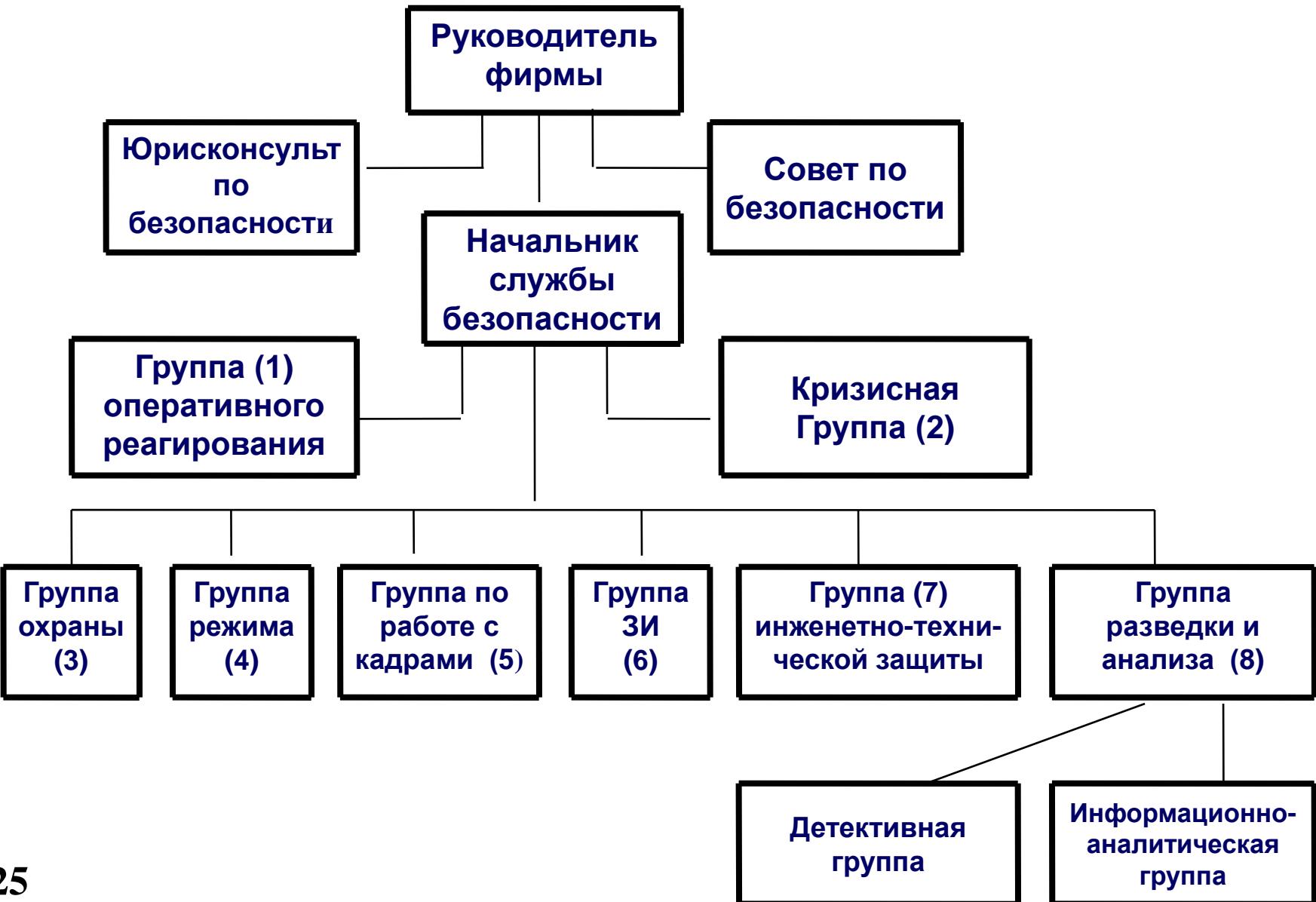
Задачи службы безопасности

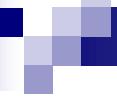
- 1. Определение сведений, составляющих КТ; лиц, имеющих к ним доступ; предприятий - партнеров на которых возможна утечка общих секретов.**
- 2. Выявление лиц и предприятий, проявляющих интерес к КТ предприятия.**
- 3. Разработка системы защиты документов с грифом КТ.**
- 4. Определение уязвимых участков на предприятии, аварии или сбои в работе которых могут нанести урон предприятию.**
- 5. Планирование, обоснование и организация мероприятий по защите экономической информации (техническое оснащение, подготовка кадров).**
- 6. Взаимодействие с ОВД.**

СБ для сохранения КТ принимает меры по

- **максимальному ограничению** круга лиц, допускаемых к КТ;
 - **физической сохранности документов,** содержащих такие сведения;
 - **обработки информации с грифом «КТ» на защищенных ЭВМ;**
 - **внесению требований** по конфиденциальности конкретной информации в договоры с внутренними и внешнеторговыми партнерами,
- а также проводит другие мероприятия по решению руководства.**

Структура службы безопасности



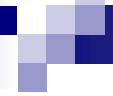


Служба безопасности должна быть готова к возникновению кризисных ситуаций

Кризисная группа создается в структуре системы безопасности фирмы для быстрого преодоления чрезвычайных ситуаций.

В состав группы входят ключевые фигуры фирмы: директор, руководители подразделений, филиалов, служб, гл. бухгалтер, юрист и др.

Деятельность этой группы тщательно планируется, а вся информация о ней должна быть конфиденциальной и максимально защищена.



Кризисной группой разрабатываются следующие **виды планов действий:**

- при угрозе взрыва;
- при захвате заложников или похищении сотрудников фирмы;
- при вымогательстве;
- при нападении на сотрудников и помещения фирмы;
- при природных и техногенных катастрофах и т.п.

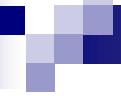
Кризисные планы составляются не более чем в 2-3 экз. и хранятся у руководителя и начальника СБ.

Частным детективам запрещается

**проведение оперативно-розыскных мероприятий и
использование специальных и иных технических средств,
предназначенных для негласного получения информации.**

Перечень специальных технических средств (СТС),
утвержденных постановлением Правительства РФ от
1 июля 1996 г. № 770:

- 1. СТС для негласного получения и регистрации
акустической информации.**
- 2. СТС для негласного визуального наблюдения и
документирования.**
- 3. СТС для негласного прослушивания телефонных
переговоров.**
- 4. СТС для негласного перехвата и регистрации информации
с технических каналов связи.**



- 5. СТС для негласного контроля почтовых сообщений и отправлений.**
- 6. СТС для негласного исследования предметов и документов.**
- 7. СТС для негласного проникновения и обследования помещений, транспортных средств и других объектов.**
- 8. СТС для негласного контроля за перемещением транспортных средств и других объектов.**
- 9. СТС для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи.**
- 10. СТС для негласной идентификации личности.**

Ответственность за данные нарушения указана в статьях УК РФ.

УК РФ. Статья 203. Превышение полномочий частным детективом или работником частной охранной организации, имеющим удостоверение частного охранника, при выполнении ими своих должностных обязанностей

1. Совершение частным детективом или работником частной охранной организации действий, выходящих за пределы полномочий, установленных законодательством РФ, и повлекших существенное нарушение прав и законных интересов граждан, организаций или государства, -
наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо ограничением свободы на срок до двух лет,

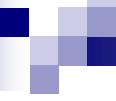
либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.

2. То же деяние, совершенное с применением насилия или с угрозой его применения либо с использованием оружия или специальных средств и повлекшее тяжкие последствия, -

наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Контрольные вопросы

- 1. Каким законом регулируются вопросы создания и деятельности частных СБ?**
- 2. Кем выдаются лицензии на осуществление частной детективной и охранной деятельности?**
- 3. Какое оружие и специальные средства могут применяться при осуществлении частной охранной деятельности?**
- 4. Могут ли частные охранники использовать специальные технические средства, предназначенные для негласного получения информации?**
- 5. Правовая ответственность за превышение полномочий служащими частных охранных или детективных служб.**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 5.1

- 1. Каким законом регулируются вопросы создания и деятельности частных СБ?**
- 2. Кем выдаются лицензии на осуществление частной детективной и охранной деятельности?**
- 3. Какое оружие и специальные средства могут применяться при осуществлении частной охранной деятельности?**
- 4. Могут ли частные охраники использовать специальные технические средства, предназначенные для негласного получения информации?**
- 5. Правовая ответственность за превышение полномочий служащими частных охранных или детективных служб.**

5.2. Правовые основы использования технических средств сбора и защиты информации

К техническим средствам сбора информации относятся:

1. Основные технические средства:

- телефоны городской, внутренней и сотовой связи;**
- селекторная связь;**
- ПК и сети ПЭВМ;**
- копировальная техника.**

Способы сбора информации с использованием телефона и линий связи

Переизлучение самой конструкции аппарата.

Старые кнопочные аппараты переизлучали информацию в СВ, КВ и УКВ на десятках частот на R до 200 м.

Утечка по звонковой цепи ТЛФ при электроакустическом преобразовании при неснятой трубке (микрофонный эффект).

Подача ВЧ колебаний (от 150 кГц) на один провод, а с другого снимаются модулированные речью колебания (трубка не снята). Дальность съема информации этими способами - несколько десятков метров.

За счет наводки в проводе, параллельном телефонному. Датчик может быть на расстоянии до 20 см от самого провода. Способ трудно обнаружить.

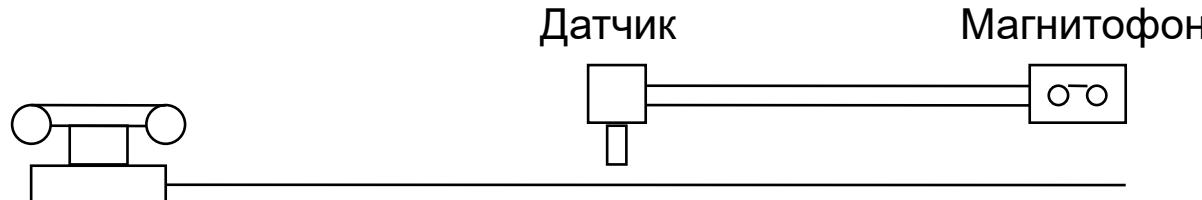


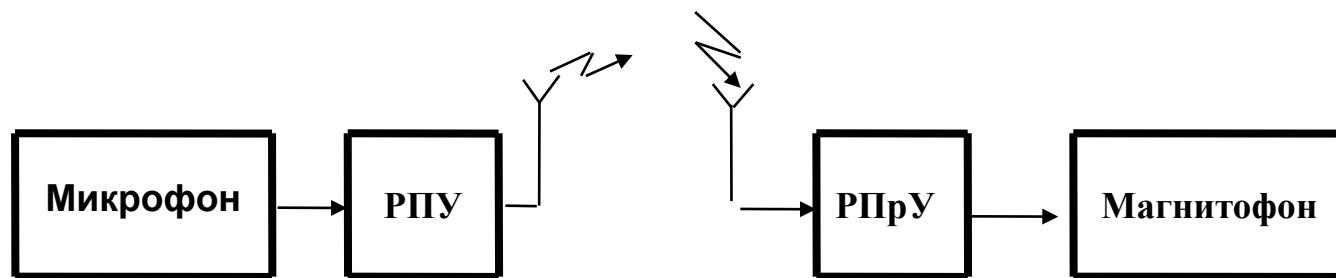
Схема снятия информации с телефонной линии

2. Вспомогательные технические средства и системы

- телевизор, магнитофон и др. виды бытовой радиоэлектроники;
- датчики охраны и пожарной сигнализации;
- кондиционер;
- штатное электрооборудование и сети газификации помещения.

3. Специальные технические средства сбора информации

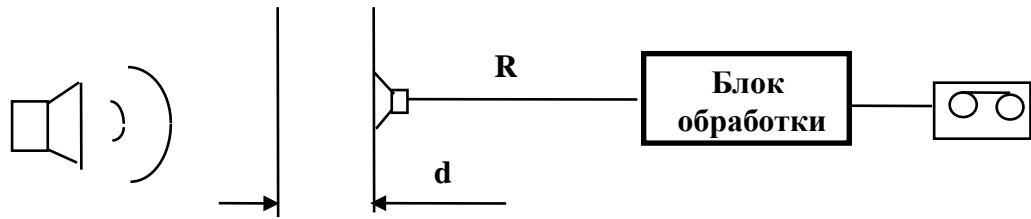
Радиомикрофон (жучок)



Структурная схема подслушивающего устройства

Стетоскоп

Прослушивание через резонирующие перегородки - стены, стекла, батареи отопления.

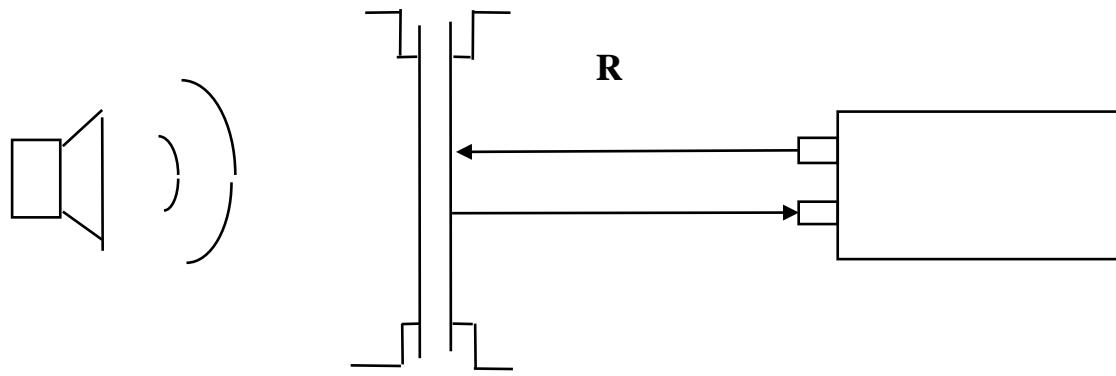


Структурная схема использования стетоскопа.

При d до 1м и R до 25 м.

d - толщина стены или балки

Лазерный локатор



**Структурная схема использования лазерного локатора.
При R до 600 м.**

Направленный микрофон

Информация по звуковому каналу считывается на расстоянии до 150 м.

Миниатюрные видео- и фотокамеры

Миниатюрные телекамеры размещенные в корпусе наручных часов, замаскированые под винт, авторучку и т.п.

Оборудование для приема побочного ЭМ излучение элементов ПК

Излучение исходит от: монитора, центрального процессора, клавиатуры, принтера, цепи питания.

Диапазон излучения от десятков кГц до сотен мГц и R до 1000 м от ПК.

Оборудование для прослушивания каналов мобильной связи

Технические средства защиты и противодействия

Средства для «контршпионажа» помогают «очистить» помещения и телефоны от всевозможных закладок или их нейтрализовать.

К таким средствам относятся.

1. Устройства поиска и обнаружения активных технических устройств и ПЭМИН (детекторы, сканеры-приемники, детекторы магнитофонов, анализаторы спектра).

Детекторы «жучков» и видеокамер изготавливаются в виде авторучки, пачки сигарет со светодиодным индикатором. Радиус действия - несколько метров.

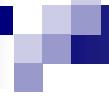
Карманный детектор подслушивающих "жучков" и скрытых видеокамер определяет точное местонахождения средств нелегального съема аудио и видео информации с передачей данных по радиоканалу.

Индикаторы радиоизлучения
в виде широкополосных приемников или
сканирующих детекторов (0,5-3000 МГц).

Нелинейные локаторы - находят пассивные и активные устройства, содержащие полупроводниковые и др. нелинейные элементы.

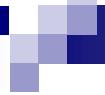
2. Средства обеспечения скрытности обмена информации

Скремблер - шифровальное средство, предназначенное для защиты информации от непосредственного прослушивания за счет: преобразование аналоговых параметров речи (временная или частотная перестановка сигнала) или цифрового шифрования.



3. Устройства нейтрализации средств съема информации

- Передатчики активных помех (в т.ч. прицельных)
- Генераторы шумов
- Устройства защиты от подслушивания через телефонную сеть
- Индикаторы субъектов и системы ограничения доступа с использованием паролей, ключей, биометрических систем (по отпечаткам пальцев, по голосу, по сетчатки глаз)

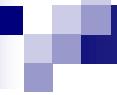


4. Программные и криптографические средства защиты

Программные средства защиты реализуются путем применения специальных программ, включенных в состав программного обеспечения АС и реализующих защиту баз данных и программ обработки конфиденциальной информации.

Используются: пароли, антивирусные программы, электронная подпись, защищенные документы.

Криптографические средства основаны на преобразовании математическими методами какого - либо сообщения.



5. Новые средства:

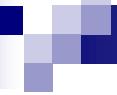
- **устройства, реагирующие на свет** (подающие сигнал при открытии ящика стола), светочувствительные покрытия, наносимые на документы
- **маркеры - красители** не смывающиеся в течение недели, защищающие от ксерокопирования, дурнopalхнущие
- **вязкая пена**
- **лазерные ослепители** (фонари)

Детекторы лжи для мобильных телефонов

Устройство может подключаться к сотовому телефону и оценивать правдивость собеседник отличает различные типы состояния и определяет, говорит ли человек правду, сильно возбужден, пытается слегка хитрить или просто врет. Разработчики заявляют, что точность мобильного полиграфа составляет почти 85%.

Услуга компании KTF на базе технологии Nemesysco.

Человеческая речь проходит через датчики, определяющие ее эмоциональную насыщенность. В конце разговора обладатель детектора лжи получает график, демонстрирующий сомнительные моменты беседы и делает соответствующие выводы.



Правовая защита информации, циркулирующей в телефонных и др. линиях связи

Конституция РФ (ст. 23, 24).

Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.
Ограничение этого права допускается только на основании судебного решения (ст. 23).

Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается (ст. 24).

УК РФ Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

- 1. Нарушения прав, указанных в 23 ст. Конституции РФ** наказываются штрафом до 80 тыс. руб., либо исправительными работами до 1 года.
- 2. Те же действия, совершенные лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации**

наказываются штрафом до 300 тыс. руб., либо лишением права занимать определенные должности на срок до 5 лет, либо арестом на срок до 4 месяцев, либо лишением свободы на срок от одного года до четырех лет.

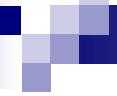
3. Незаконные производство, сбыт или приобретение специальных технических средств, предназначенных для негласного получения информации, -

наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо ограничением свободы на срок до трех лет, либо **лишением свободы на срок до трех лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

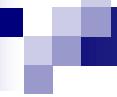
Регулирование деятельности, связанной со специальными техническими средствами

Указ Президента РФ №21 от 9.01 96г. «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в РФ и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации» постановляет возложить на ФСБ:

- **выдачу разрешений на деятельность и контроль использования в области специальных технических средств, предназначенных для негласного получения информации**



- лицензирование деятельности не уполномоченных на осуществление оперативно-розыскной деятельности физических и юридических лиц, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввозом в РФ и вывозом за ее пределы специальных технических средств, предназначенных для негласного получения информации, а также сертификацию, регистрацию и учет таких специальных технических средств;
- выявление и пресечение случаев проведения оперативно-розыскных мероприятий и использования специальных и иных технических средств, разработанных, приспособленных, запрограммированных для негласного получения информации, неуполномоченными лицами.

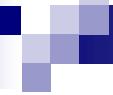


**Постановлением Правительства от 1.07.96г. №770 введено
“Положение о лицензировании деятельности физических и
юридических лиц, не уполномоченных на осуществление
оперативно-розыскной деятельности, связанной с
разработкой, производством, реализацией,
приобретением в целях продажи, ввоза в РФ и вывоза за
ее пределы СТС (специальных технических средств) ”.**

**В постановлении регламентируются деятельность,
связанная с использованием СТС, предназначенных для
негласного получения информации.**

Лицензированию подлежат следующие виды деятельности:

- разработка и производство СТС;
- реализация СТС;
- приобретение СТС в целях продажи, ввоза и вывоза из РФ.



Регламентируется также деятельность, связанная с применением радиоэлектронным средствам (РЭС).

Постановлением Правительства РФ от 5.06.94г. №643 утверждено “Положение о порядке изготовления, ввоза в РФ и использования на территории РФ радиоэлектронных средств”.

В данном постановлении к РЭС относятся:

- **радиостанции**
- **системы радионавигации**
- **системы кабельного телевидения**
- **другие устройства с рабочей частотой выше 9 кГц.**

Литература

- 1.Шпионские штучки. Под ред. Золоторева С.А. Справочное пособие. Лань, 1996.
- 2.Технические средства защиты. /Конфидент. Защита информации, №1. 1994.
- 3.Сугубо конфиденциально. /Коммерсант, №40 за октябрь 1994г.
- 4.Ярочкин В.И. Служба безопасности коммерческого предприятия. М.: Ось-89. 1995.
- 5.О.Панин. Служба безопасности и ее роль в обеспечении комплексной защиты предприятия // «Безопасность, достоверность, информация», №2 (53), 2004, с.24-27,

Контрольные вопросы

- 1. Назовите основные и вспомогательные технические средства утечки информации.**
- 2. Какие технические средства используются для защиты от СТС негласного получения информации?**
- 3. Ответственность за нарушения конституционного права на личную тайну (тайна переписки телефонных переговоров и др. сообщений).**
- 4. Ответственность за незаконное использование СТС.**
- 5. Кто занимается вопросами лицензирования и контроля в области СТС получения информации?**
- 6. Какие виды деятельности подлежат лицензированию в области СТС?**
- 7. Какими документами регулируется деятельность, связанная с использованием радиоэлектронных средств и СТС?**

Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

К.т.н.

Струков Владимир Ильич

Вопросы к разделу 5.2

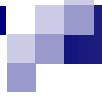
- 1. Назовите основные и вспомогательные технические средства утечки информации.**
- 2. Какие технические средства используются для защиты от СТС негласного получения информации?**
- 3. Ответственность за нарушения конституционного права на личную тайну (тайна переписки телефонных переговоров и др. сообщений).**
- 4. Ответственность за незаконное использование СТС.**
- 5. Кто занимается вопросами лицензирования и контроля в области СТС получения информации?**
- 6. Какие виды деятельности подлежат лицензированию в области СТС?**
- 7. Какими документами регулируется деятельность, связанная с использованием радиоэлектронных средств и СТС?**

6. Лицензирование и сертификация в области ЗИ

6.1. Правовая основа системы лицензирования и сертификации в РФ

Для обеспечения защиты ГТ и СТ (в важных для страны областях) действует Государственная система защиты информации в РФ (ГСЗИ), которая включает:

- совокупность органов (ФСБ, ФСТЭК, СБ), сил и средств, осуществляющих деятельность в области защиты информации (ЗИ);**
- систему лицензирования деятельности в области ЗИ;**
- систему сертификации средств ЗИ;**
- систему подготовки и переподготовки специалистов в области ЗИ.**



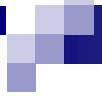
Лицензирование

- это **процесс** передачи или получения в отношении физических или юридических лиц прав на проведение определенных работ.

Получить право или разрешение на определенную деятельность может не каждый субъект, а только отвечающий определенным критериям в соответствии с правилами лицензирования.

Лицензия

- **документ**, дающий право на осуществление указанного вида деятельности в течении определенного времени.



Перечень видов деятельности в области ЗИ, на которые выдаются лицензии, определен **Постановлением Правительства РФ - “О лицензировании отдельных видов деятельности”** от 24.12.94 №1418 к ним, в частности, относится **разработка, производство, реализация и сервисное обслуживание:**

- шифровальных средств;
- защищенных систем телекоммуникаций;
- программных средств;
- специальных технических средств ЗИ;

а также подготовка и переподготовка кадров.

Сертификация

- это **подтверждение соответствия** продукции или услуг установленным требованиям или стандартам.

Сертификат

- **документ**, подтверждающий соответствие средства ЗИ требованиям по безопасности информации.

Законодательной и нормативной базой лицензирования и сертификации в области ЗИ являются

Законы РФ:

- “О государственной тайне” от 21.07.93 №5485-1;
- “О техническом регулировании” от 27 декабря 2002 г. N 184-ФЗ
- “О лицензировании отдельных видов деятельности”, от 8.08 2001г. №128 (ред. от 11.03.2003г. №32);
- “О защите прав потребителей” от 07.02.92 №2300-1;

Постановления Правительства РФ:

- “О лицензировании отдельных видов деятельности” от 24 12 94 №1418;
- “О лицензировании деятельности предприятий...” от 15.04.95 №333;
- “О сертификации средств ЗИ” от 26.06.95 №608.
- “О лицензировании... от 27.05.2002 №348.
- “О лицензировании... от 30.04.2002 №290, (ред. №64 от 6.02.2003).

А также Указы Президента РФ, и ряд других подзаконных актов.

6.2. Лицензирование деятельности по защите ГТ

Общие нормы, устанавливающие порядок организации и осуществления этой деятельности, содержатся в статье 27 Закона "О государственной тайне".

Основные положения данной статьи:

- лицензия выдается только на основании результатов специальной экспертизы (проверки готовности организации к работе со сведениями, составляющими ГТ);
- в структуре организации должно быть подразделение по защите ГТ и специально подготовленные сотрудники;
- организация должна иметь сертифицированные средства ЗИ;
- необходима государственная аттестация руководителей организаций, ответственных за защиту государственных секретов.

Постановлением Правительства РФ №333 утверждено

**Положение о лицензировании деятельности
предприятий, в котором установлено, что:**

**-лицензия разрешает осуществление конкретного вида
деятельности в течение установленного срока на всей
территории Российской Федерации, а также в
учреждениях Российской Федерации, находящихся за
границей;**

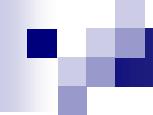
**-органами, уполномоченными на ведение лицензионной
деятельности, являются:**



по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих ГТ
- ФСБ, СВР(за рубежом);

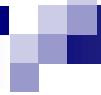
на право проведения работ, связанных с созданием средств защиты информации
- ФСТЭК, ФСБ в пределах их компетенции;

на право осуществления мероприятий и (или) оказания услуг в области защиты ГТ
– ФСБ и ее территориальные органы, ФСТЭК, СВР (в пределах их компетенции).



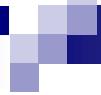
Лицензирование деятельности предприятий ФСБ, МО, Федеральной пограничной службы Российской Федерации, СВР и ФСТЭК по допуску к проведению работ, связанных с использованием сведений, составляющих ГТ, осуществляется руководителями министерств и ведомств РФ, которым подчинены указанные предприятия.

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но не может быть менее трех и более пяти лет.



Основанием для отказа в выдаче лицензии является:

- наличие в представленных документах недостоверной или искаженной информации;**
- отрицательное заключение экспертизы;**
- отрицательное заключение по результатам государственной аттестации руководителя предприятия.**



Специальные экспертизы предприятий
выполняются по следующим направлениям:

- режим секретности;
- противодействие иностранной технической разведке;
- защита информации от утечки по техническим каналам.

**Экспертные комиссии формируются при ФСБ,
ФСТЭК и их органах на местах и
аттестационных центрах.**

Принципы лицензирования:

1. Лицензирование в области защиты ГТ является обязательным.
2. Деятельность в области ЗИ лиц, не прошедших лицензирование, запрещена (с применением соответствующих статей ГК и УК к нарушителям).
3. Лицензии на право деятельности в области защиты ГТ выдаются только юридическим лицам независимо от организационно - правовой формы (физические лица не в состоянии удовлетворить указанным требованиям).
4. Лицензии выдаются только предприятиям, зарегистрированным на территории РФ на основании специальной экспертизы заявителя.



**Для получения лицензии предприятие обязано предъявить
следующий перечень документов.**

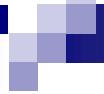
К заявлению на получение лицензии необходимо приложить
следующие документы:

- копия свидетельства о государственной регистрации предприятия;
- копии учредительных документов, заверенных нотариусом;
- копии документов на право собственности или аренды имущества, необходимого для ведения заявленной деятельности;
- справка налогового органа о постановке на учет;
- представление органов государственной власти РФ с ходатайством о выдаче лицензии;
- документ, подтверждающий оплату рассмотрения заявления.

Проведение экспертизы осуществляется экспертными комиссиями Лицензионного центра либо Аттестационными центрами.

Например, коммерческому банку, претендующему на получение лицензии на эксплуатацию шифровальных средств для защиты конфиденциальной информации предъявляются требования по:

- **наличию и составу необходимых аппаратно-программных средств и помещений;**
- **размещению, охране и специальному оборудованию помещений**, в которых находятся средства криптографической ЗИ;
- **обеспечению режима и порядка доступа** к средствам криптографической ЗИ;
- **обеспечению необходимой технической и эксплуатационной документацией;**
- **уровню квалификации и подготовленности** специалистов в области защиты и эксплуатации АС;
- **режиму эксплуатации и хранения** средств криптографической ЗИ.



Система лицензирования обеспечивает в отношении АС выполнение 3 основных требований к защищаемой информации:

-доступность;

-целостность;

-конфиденциальность.

Государственная аттестация руководителей ответственных за защиту ГТ

Основная цель государственной аттестации –
повысить компетентность руководителей в части
обеспечения сохранности сведений,
составляющих ГТ.

Документом, по организации государственной
аттестации руководителей является **Инструкция**
о порядке проведения государственной
аттестации руководителей предприятий,
учреждений и организаций, ответственных за
защиту сведений, составляющих ГТ,
утвержденная Председателем ГТК 17.10.95 г.

Государственное аттестование проводится методом собеседования аттестационной комиссии с руководителем предприятия.

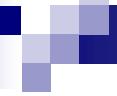
К аттестуемому предъявляются следующие требования.

Должен знать:

- законодательные акты РФ по вопросам защиты ГТ;
- нормативные документы, утверждаемые Правительством РФ, по обеспечению защиты сведений, составляющих ГТ;
- нормативно-методические документы по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, утверждаемые ФСБ и ГТК;
- перечень продукции предприятия, подлежащей защите от разведок, основные охраняемые сведения о предприятии и выпускаемой продукции;
- возможные каналы утечки информации по всему технологическому циклу разработки, изготовления и испытаний продукции предприятия;
- деловые и моральные качества сотрудников структурного подразделения предприятия по защите ГТ.

Должен уметь организовывать:

- разработку мероприятий по защите сведений о предприятии и выпускаемой продукции, составляющих ГТ, и оценку их достаточности;
- проведение анализа возможностей разведки по добыванию сведений, составляющих ГТ;
- аттестование рабочих мест по всему технологическому циклу разработки, изготовления и испытания продукции;
- комплексный контроль выполнения принимаемых мер по защите сведений, составляющих ГТ.



Быть ознакомленным:

- с государственной системой лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих ГТ, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите ГТ;
- с возможностями иностранных разведок по добыванию сведений, составляющих ГТ;
- с методиками контроля выполнения норм противодействия иностранным техническим разведкам.

6.3. Сертификация средств защиты информации

Национальный орган по сертификации определяется Правительством РФ.

В настоящее время эти функции выполняет **Федеральное агентство по техническому регулированию и метрологии (ФАТРиМ)**.

В 1994 г. Были утверждены “Правила по проведению сертификации в РФ”, в соответствии с которыми целями сертификации являются:

- **создание условий** для деятельности предприятий и предпринимателей на товарном рынке РФ и участия в международной торговли;
- **содействие потребителям** в компетентном выборе продукции;
- **содействие экспорту** и повышение конкурентоспособности продукции;
- **защита потребителя** от недобросовестности изготовителя (продавца, исполнителя);
- **контроль безопасности** продукции для окружающей среды, жизни и имущества;
- **подтверждение** показателей **качества** продукции, заявленных изготовителями.

Организация сертификации средств ЗИ

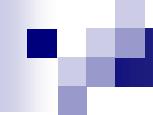
возлагается на ФСТЭК, ФСБ и МО в соответствии с функциями, возложенными на них законодательством РФ.

Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ.

Положение о сертификации средств ЗИ

утверждено постановлением Правительства РФ от 25.06.95 г. № 608 (в ред. ПП РФ N 509 от 23.04.96) и зарегистрировано Госстандартом России в

Государственном реестре 20 марта 1995 г. (Свидетельство № Р0СС RU. 0001. 01БИ00).



Обязательной сертификации (в соответствии с этим Положением) подлежат средства, в том числе иностранного производства, предназначенные для защиты информации, составляющей ГТ, и другой **информации с ограниченным доступом**, а также средства, использующиеся в управлении экологически опасными объектами.

В остальных случаях сертификация носит **добровольный** характер (добровольная сертификация) и осуществляется по инициативе разработчика, изготовителя или потребителя средства защиты информации.

Принципы сертификации:

1. Сертификация изделий, обеспечивающих защиту ГТ является обязательной.
2. Обязательность использования криптографических алгоритмов, являющихся стандартами.
3. Принятие на сертификацию изделий только от заявителей, имеющих лицензию.

В соответствии с вышеназванными документами, государственным организациям и предприятиям запрещено использование в информационных системах шифровальных средств, не имеющих сертификата.

Кроме этого в области информационных технологий действуют системы добровольной сертификации банковских технологий (МЕКАС) и средств связи.

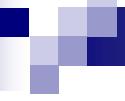
Порядок сертификации:

1. В Центральный орган по сертификации подается заявление и полный комплект технической документации.
2. Центральный орган назначает испытательный центр (лабораторию) для проведения испытания.
3. Испытания проводятся на основании хозяйственного договора между заявителем и испытательным центром.
4. Сертификация (экспертиза материалов и подготовка документов для выдачи) осуществляется Центральным органом.

Сертификат выдается на срок до 5 лет.

Контрольные вопросы

- 1. Укажите основные элементы организационной основы системы обеспечения информационной безопасности РФ.**
- 2. Какие виды деятельности в области защиты информации подлежат лицензированию?**
- 3. Порядок лицензирования, срок действия лицензии.**
- 4. При каких организациях созданы системы сертификации в РФ?**
- 5. Порядок и требования при осуществлении сертификации средств защиты информации.**
- 6. В каких случаях сертификация носит добровольный характер?**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 6.1

- 1. Укажите основные элементы организационной основы системы обеспечения информационной безопасности РФ.**
- 2. Какие виды деятельности в области защиты информации подлежат лицензированию?**
- 3. Порядок лицензирования, срок действия лицензии.**
- 4. При каких организациях созданы системы сертификации в РФ?**
- 5. Порядок и требования при осуществлении сертификации средств защиты информации.**
- 6. В каких случаях сертификация носит добровольный характер?**

6.4. Лицензирование и сертификация в области защиты конфиденциальной информации

Лицензирование деятельности в области защиты конфиденциальной информации основано на Законе РФ «О лицензировании отдельных видов деятельности» от 8 августа 2001 г. N 128-ФЗ (ред. от 4 мая 2011 г. N 99-ФЗ).

Действие данного закона не распространяется на следующие виды деятельности, связанные с ЗИ:

- ▶ **деятельность, связанная с защитой государственной тайны;**
- ▶ **деятельность в области связи;**
- ▶ **использование результатов интеллектуальной деятельности.**

В соответствии законом лицензированию подлежат
следующие виды деятельности в области ЗИ:

- ▶ **разработка, производство, распространение, техническое обслуживание и предоставление услуг в области шифрования информации;** шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- ▶ **деятельность по выдаче сертификатов ключей ЭЦП,** регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

- ▶ **деятельность по выявлению электронных устройств негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);**
- ▶ **деятельность по разработке и (или) производству средств защиты конфиденциальной информации;**
- ▶ **деятельность по технической защите конфиденциальной информации;**
- ▶ **разработка, производство, реализация и приобретение в целях продажи СТС, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.**

В новой редакции закона «О лицензировании отдельных видов деятельности» добавлены следующие виды деятельности:

- ▶ **деятельность по изготовлению экземпляров аудиовизуальных произведений, программ для ЭВМ, баз данных и фонограмм на любых видах носителей;**
- ▶ **образовательная деятельность ;**
- ▶ **частная охранная деятельность;**
- ▶ **частная детективная (сыскная) деятельность;**
- ▶ **оказание услуг связи.**

Заявление о предоставлении лицензии и прилагаемые к нему документы соискатель лицензии вправе направить в лицензирующий орган как **почтовым отправлением**, так и в **форме электронного документа**, подписанного ЭЦП.

В этом случае лицензирующий орган направляет соискателю **лицензии в форме электронного документа**, подписанного ЭЦП.

На каждый вид деятельности предоставляется **лицензия**, которая действует **бессрочно**.

В 4-х последних случаях срок ее действия может устанавливаться федеральными законами (**ст. 1**).

В ст. 14 закона дан порядок принятия решения о предоставлении лицензии или об отказе.

Решение принимается в течении 45 дней.

В течении 3-х дней после подписания, лицензия вручается или направляется по почте лицензиату.

Проводятся плановые проверки лицензиата

Основания для их проведения:

- истечение 1 года после предоставления лицензии,
- истечение 3-х лет после последней проверки.

А также внеплановые проверки.

**Постановление Правительства РФ от 3.02.2012 г. № 79
утвердило "Положение о лицензировании деятельности
по технической защите конфиденциальной
информации.**

Положение определяет **порядок лицензирования** данной
деятельности, осуществляемой юридическими лицами и
индивидуальными предпринимателями.

Под **технической защитой конфиденциальной
информации (ТЗКИ)** понимается комплекс мероприятий по
ее защите от несанкционированного доступа в целях ее
**уничтожения, искажения или блокирования доступа к
ней.**

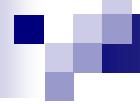
Лицензирование работ по ТЗКИ осуществляет **ФСТЭК**.

Лицензированию подлежат **следующие виды работ и услуг:**

- ▶ **контроль защищенности** конфиденциальной информации от утечки **по техническим каналам**
- ▶ **контроль защищенности** конфиденциальной информации от НСД в средствах и системах информатизации
- ▶ **сертификационные испытания** на соответствие требованиям по безопасности информации продукции
- ▶ **аттестационные испытания и аттестация** на соответствие требованиям по защите информации
- ▶ **проектирование в защищенном исполнении** средств и систем информатизации
- ▶ **установка, монтаж, испытания, ремонт** средств защиты информации

Лицензионные требования к соискателю

- ▶ **наличие в штате соискателя лицензии специалистов, имеющих высшее профессиональное образование в области технической защиты информации**
- ▶ **наличие у соискателя помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации**
- ▶ **наличие производственного, испытательного и контрольно-измерительного оборудования, прошедшего метрологическую поверку (калибровку), маркирование и сертификацию**



- ▶ **наличие** средств контроля защищенности информации от несанкционированного доступа
- ▶ **использование АС**, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших сертификацию
- ▶ **использование программ для ЭВМ и баз данных на основании договора с их правообладателем**
- ▶ **наличие технической документации** необходимой для выполнения работ
- ▶ **наличие** системы производственного контроля

Для получения лицензии соискатель представляет в лицензирующий орган следующие документы:

- ▶ **заявление** о предоставлении лицензии
- ▶ **копии документов**, подтверждающих квалификацию специалистов по защите информации (дипломов, удостоверений, свидетельств)
- ▶ **копии документов**, подтверждающих право собственности, на помещения, предназначенные для осуществления лицензируемой деятельности, либо копии договоров аренды указанных помещений
- ▶ **копии аттестатов соответствия** защищаемых помещений требованиям безопасности информации

- ▶ **копии технического паспорта АС** с приложениями, акта классификации автоматизированной системы по требованиям безопасности информации, и др.
- ▶ **копии документов**, подтверждающих право на программы для ЭВМ и базы данных
- ▶ **сведения о наличии производственного и контрольно-измерительного оборудования**, средств защиты информации и средств контроля защищенности информации
- ▶ **сведения об имеющихся у соискателя нормативных правовых актах**, и методических документах по вопросам технической защиты информации

Постановление Правительства от 3.03.2012 г. N 171
утвердило "Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации".

Положение определяет **порядок лицензирования данной деятельности, осуществляемой юридическими лицами и индивидуальными предпринимателями.**

Лицензирование деятельности **осуществляет - ФСТЭК,**
а в части средств защиты конфиденциальной информации,
устанавливаемых на объектах Администрации Президента
РФ, Совета Безопасности РФ, Федерального Собрания РФ,
Правительства РФ, Конституционного, Верховного и
Высшего Арбитражного Суда РФ - **ФСБ.**

Лицензированию подлежит разработка и производство
следующих средств защиты конфиденциальной
информации:

- **технических средств защиты информации**
- **защищенных технических средств обработки**
информации
- **технических средств контроля эффективности мер**
защиты информации
- **программных (программно-технических) средств защиты**
информации
- **защищенных программных (программно-технических)**
средств обработки информации
- **программных (программно-технических) средств**
контроля защищенности информации

Лицензионные требования ФСТЭК к лицензиату:

- а) наличие в штате соискателя специалистов, имеющих высшее профессиональное образование в области технической защиты информации;**
- б) наличие у соискателя помещений для осуществления лицензируемой деятельности, принадлежащих ему на праве собственности или на ином законном основании;**
- в) выполнение требований конструкторской, программной и технологической документации в области технической защиты информации;**
- г) соответствие помещений, техническим нормам и требованиям по технической защите информации;**
- д) наличие нормативных правовых актов и методических документов по вопросам разработки средств защиты информации в соответствии с перечнем, ФСТЭК.**

Лицензионные требования ФСБ к лицензиату:

- а) выполнение нормативных правовых актов, регламентирующих осуществление лицензируемой деятельности;**
- б) выполнение режима конфиденциальности при обращении со сведениями, которые ему доверены или стали известны в ходе служебной деятельности;**
- в) наличие условий, предотвращающих несанкционированный доступ к средствам защиты конфиденциальной информации, обеспечивающих хранение нормативной и эксплуатационной документации, инсталляционных дискет и дистрибутивов программных и программно-аппаратных средств защиты конфиденциальной информации в металлических шкафах (хранилищах, сейфах);**

Лицензионные требования ФСБ к лицензиату:

- г) соответствие помещений требованиям технической и технологической документации на используемое оборудование;**
- д) соответствие оборудования установленным требованиям;**
- е) аттестация средств обработки информации, в соответствии с требованиями по защите информации;**
- ж) выполнение требований конструкторской, программной и технологической документации, средств защиты конфиденциальной информации;**

Лицензионные требования ФСБ к лицензиату:

- з) наличие системы учета изменений, внесенных в техническую и конструкторскую документацию на производимую продукцию, и системы учета готовой продукции;**
- и) наличие у руководителя соискателя документа о высшем профессиональном образовании в области технической защиты информации, а также производственного стажа в области лицензируемой деятельности не менее 5 лет;**
- к) наличие у инженерно-технического персонала, документа о высшем образовании или профессиональной подготовке со специализацией, соответствующей выполняемым работам.**

Для получения лицензии соискатель лицензии направляет в лицензирующий орган следующие документы:

- а) заявление о предоставлении лицензии и другие указанные в законе документы;**
- б) копии документов, подтверждающих квалификацию специалистов;**
- в) копии документов, подтверждающих право собственности, либо копии договоров аренды помещений;**
- г) копии документов, подтверждающих право на используемые программы для электронно-вычислительных машин и базы данных;**

Для получения лицензии соискатель лицензии направляет в лицензирующий орган следующие документы:

- д) сведения о наличии необходимого производственного, испытательного и контрольно-измерительного оборудования;**
- е) сведения об имеющихся у соискателя нормативных правовых актах, по вопросам разработки и производства средств защиты информации.**

Лицензирующий орган принимает решение о предоставлении или об отказе в предоставлении лицензии в срок, не превышающий 45 дней с даты поступления в лицензирующий орган заявления.

**Приказом ФСБ от 1 апреля 2009 г. № 123 утвержден
регламент ФСБ РФ по исполнению государственной
функции по лицензированию деятельности
по разработке и (или) производству средств защиты
конфиденциальной информации.**

**Регламент определяет сроки и последовательность
действий по лицензированию деятельности по разработке
и (или) производству средств защиты конфиденциальной
информации.**

Схема последовательности действий

- 1.Прием лицензирующим органом заявления о предоставлении(продлении срока действия, переоформлении документа, подтверждающего наличие) лицензии**
- 2.Проверка лицензирующим органом полноты и достоверности сведений о соискателе лицензии и возможности выполнения соискателем лицензии лицензионных требований и условий**
- 3.Принятие лицензирующим органом решения о предоставлении или об отказе в предоставлении лицензии**
- 4.Уведомление лицензирующим органом соискателя лицензии о предоставлении или об отказе в выдаче лицензии**
- 5.Выдача лицензирующим органом соискателю лицензии документа, подтверждающего наличие лицензии (в случае принятия решения о предоставлении лицензии)**
- 6.Занесение сведений о лицензиате в реестр лицензий**

Грубыми нарушениями лицензионных требований и условий являются:

невыполнение лицензиатом режима конфиденциальности при обращении со сведениями, которые ему доверены или стали известны в ходе служебной деятельности;

отсутствие у руководителя лицензиата документа о высшем профессиональном образовании в области технической защиты информации, а также производственного стажа в области лицензируемой деятельности не менее 5 лет;

отсутствие у инженерно-технического персонала, осуществляющего работы в области лицензируемой деятельности, документа о высшем образовании или профессиональной подготовке со специализацией, соответствующей выполняемым работам.

Сертификация средств защиты конфиденциальной информации проводится в соответствии с Положением "О сертификации средств защиты информации", утвержденным ПП РФ от 23.04.96 N 509 (с изменениями от 17 декабря 2004 года N 808).

Положение устанавливает **порядок сертификации средств защиты информации** в РФ и ее учреждениях за рубежом.

Сертификационные испытания средств защиты в рамках данной системы сертификации предусматривают **мероприятия по проверке соответствия этих средств формальным базовым требованиям** по обеспечению безопасности информации, изложенным в нормативных документах ФСТЭК.

В Ассоциации "ЕВРААС" действует **Система добровольной сертификации средств информационных технологий по требованиям информационной безопасности "АйТиСертифика"** (Система зарегистрирована в Госстандарте России 1 июля 2003 г., регистрационный № РОСС RU.М089ИТ00).

Область деятельности Системы сертификации распространяется на изделия, технологии и объекты, в отношении которых существуют требования по защите конфиденциальной информации.

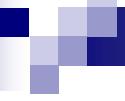
Данная система позволяет подтверждать соответствие требованиям национальных стандартов, стандартов организаций, условиям договоров и **является инструментом** для выполнения требований по сертификации продукции и услуг, в **области защиты конфиденциальной информации (включая криптографические)**.

Дополнительная литература по теме

- 1. Беззубцев О.А., Ковалев А.Н. Лицензирование и сертификация в области ЗИ. М.: МИФИ, 2002.**
- 2. Костогрызов А.И. Липаев В.В. Сертификация качества функционирования автоматизированных систем. М.: Вооружения. Политика. Конверсия. 2004.**

Контрольные вопросы

- 1. На каких правовых документах основана система лицензирования и сертификации в области защиты конфиденциальной информации?**
- 2. Порядок лицензирования деятельности по технической защите конфиденциальной информации.**
- 3. Порядок лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации.**
- 4. Лицензионные требования ФСТЭК и ФСБ к лицензиату.**
- 5. В соответствии с каким документом устанавливается порядок сертификации средств защиты информации в РФ.**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

К.Т.Н.

Струков Владимир Ильич

Вопросы к разделу 6.2

- 1. Укажите основные элементы организационной основы системы обеспечения информационной безопасности РФ.**
- 2. Какие виды деятельности в области защиты информации подлежат лицензированию?**
- 3. Порядок лицензирования, срок действия лицензии.**
- 4. Организационная структура системы сертификации в области защиты информации.**
- 5. При каких организациях созданы системы сертификации в РФ?**
- 6. Порядок и требования при осуществлении сертификации средств защиты информации.**
- 7. В каких случаях сертификация носит добровольный характер?**
- 8. На каких документах основана система лицензирования и сертификации в области защиты конфиденциальной информации?**

7. Система юридической ответственности за нарушение защиты информации

7.1. Нормы ответственности за правонарушения в информационной сфере

В законодательных актах установлены правовые нормы в отношении прав, обязанностей и ответственности субъектов, участвующих в информационном обмене.

Предметом правового регулирования в информационной сфере являются:

- создание и распространение информации;**
- формирование и использование информационных ресурсов;**
- реализация права на поиск, получение, передачу и потребление информации;**
- создание и применение информационных систем и технологий;**
- создание и применение средств информационной безопасности.**

Ответственность, возлагаемая в случаях правонарушений в информационной сфере, формулируется в различных нормативных правовых актах.

Конкретные нормы, устанавливающие ответственность за нарушения сосредоточены в Уголовном, Гражданском, Административном кодексах и в др. правовых актах.

Уголовное право регулирует отношения в области наиболее опасных правонарушений - преступлений.

Санкции за нарушение информационных правоотношений представлены в УК следующими статьями.

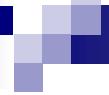
Статья 137. Нарушение неприкосновенности частной жизни.

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Статья 140. Отказ в предоставлении гражданину информации.

Статья 146. Нарушение авторских и смежных прав.

Статья 147. Нарушение изобретательских и патентных прав.



Статья 180. Незаконное использование товарного знака.

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Статья 204. Коммерческий подкуп .

Статья 272. Неправомерный доступ к компьютерной информации.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

**Статья 274. Нарушение правил эксплуатации ЭВМ,
системы ЭВМ или их сети.**

Статья 275. Государственная измена.

Статья 276. Шпионаж.

Статья 283. Разглашение государственной тайны.

**Статья 284. Утрата документов, содержащих
государственную тайну.**

7.2. Защита информации от неправомерных действий органов, занимающихся оперативно-розыскной деятельностью

Деятельность этих органов основывается на

**Законе РФ “Об оперативно-розыскной деятельности”,
от 12.08.95г. №144-ФЗ (ред. от 22.08.2004 №122-ФЗ).**

**Оперативно-розыскная деятельность (ОРД) - вид
деятельности, осуществляемый, гласно и негласно
оперативными подразделениями уполномоченных
государственных органов, в целях защиты жизни,
здравья, прав и свобод человека и гражданина,
собственности, обеспечения безопасности общества
и государства от преступных посягательств (ст. 1).**

Задачи ОРД - выявление, предупреждение, пресечение и раскрытие преступлений (в том числе установление лиц их совершающих, розыска уклоняющихся от уголовного наказания лиц и т.д.).

Принципы ОРД - законность, уважение прав и свобод личности, конспирация, сочетание гласности и негласных действий (ст. 3).

Организация и тактика проведения ОРМ (сведения об используемых силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности) составляют государственную тайну (ст. 12). В связи с этим в открытой литературе подобные сведения практически отсутствуют.

Оперативно-розыскными мероприятиями (ОРМ) предусматривается (ст. 6) проведение таких мероприятий как прослушивание телефонных переговоров и снятие информации с технических каналов связи.

В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде.

Оперативно-розыскными мероприятиями предусматривается проведение следующих мероприятий (ст. 6):

- 1. Опрос.**
- 2. Наведение справок.**
- 3. Сбор образцов для сравнительного исследования.**
- 4. Проверочная закупка.**
- 5. Исследование предметов и документов.**
- 6. Наблюдение.**
- 7. Отождествление личности.**
- 8. Обследование помещений, зданий, сооружений, участков местности и транспортных средств.**
- 9. Контроль почтовых отправлений, телеграфных и иных сообщений.**
- 10. Прослушивание телефонных переговоров.**
- 11. Снятие информации с технических каналов связи.**
- 12. Оперативное внедрение.**
- 13. Контролируемая поставка.**
- 14. Оперативный эксперимент.**

В ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде.

ОРМ, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров проводятся с использованием сил и средств органов ФСБ, ОВД и органов по контролю за оборотом наркотических и психотропных веществ.

**Ввоз в РФ и вывоз за ее пределы СТС, не
уполномоченными на осуществление оперативно-
розыскной деятельности физическими и
юридическими лицами подлежат лицензированию.**

**Разработка, производство, реализация и приобретение
в целях продажи СТС индивидуальными
предпринимателями и юридическими лицами,
осуществляющими предпринимательскую
деятельность, подлежат лицензированию (ст. 6).**

Запрещается проведение ОРМ и использование СТС, не уполномоченными на то физическими и юридическими лицами.

Органам, осуществляющим оперативно-розыскную деятельность, запрещается: разглашать личную и семейную тайну, в процессе проведения ОРМ, без согласия граждан (ст. 5).

В стране действует также Система оперативно-розыскных мероприятий – 2 (СОРМ-2), касающаяся операторов сотовой связи.

При проведении ОРМ должны соблюдаться права человека и гражданина на неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну корреспонденции (ст. 5).

Полученные в результате ОРД материалы в отношении лиц, виновность которых не доказана, хранятся 1 год, а затем уничтожаются.

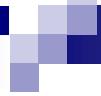
Фонограммы и другие материалы, полученные в результате прослушивания телефонных и иных переговоров лиц, в отношении которых не было возбуждено уголовное дело, уничтожаются в течение шести месяцев с момента прекращения прослушивания. Об этом уведомляется соответствующий судья.

Основания для проведения ОРМ (ст. 7):

- 1. Наличие возбужденного уголовного дела.**
- 2. Ставшие известными органам, осуществляющим ОРД, сведения о:**
 - подготавливаемых, совершаемых или совершенных противоправных действиях, лицах их совершающих, если нет достаточных данных для возбуждения уголовного дела;**
 - лицах, скрывающихся от уголовного наказания;**
 - безвестном отсутствии граждан и обнаружении неопознанных трупов;**
 - событиях или действиях, создающих угрозу безопасности РФ.**

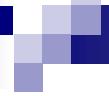


- 3.Поручения следователя, указания прокурора или определения суда по уголовным делам, находящимся в их производстве.**
- 4.Запросы других органов, осуществляющих оперативно-розыскную деятельность, по основаниям, указанным в настоящей статье.**
- 5.Постановление о применении мер безопасности в отношении защищаемых лиц.**
- 6.Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами РФ.**

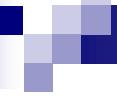


Органы, осуществляющие оперативно-розыскную деятельность, в пределах своих полномочий вправе также собирать данные, необходимые для принятия решений:

- 1. О допуске к сведениям, составляющим ГТ.**
- 2. О допуске к работам, связанным с эксплуатацией объектов, представляющих повышенную опасность для жизни и здоровья людей, а также для окружающей среды.**
- 3. О допуске к участию в оперативно-розыскной деятельности или о доступе к материалам, полученным в результате ее осуществления.**

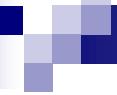


- 4. Об установлении или о поддержании с лицом отношений сотрудничества при подготовке и проведении оперативно-розыскных мероприятий.**
- 5. По обеспечению безопасности органов, осуществляющих оперативно-розыскную деятельность.**
- 6. О выдаче разрешений на частную детективную и охранную деятельность.**
- 7. По розыску лиц, скрывающихся от органов дознания.**



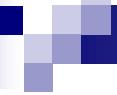
Проведение ОРМ, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации:

- 1. О признаках** подготавливаемого, совершающего или совершенного **противоправного деяния**, по которому производство предварительного следствия обязательно.
- 2. О лицах**, подготавливающих, совершающих или **совершивших противоправное деяние**, по которому производство предварительного следствия обязательно.
- 3. О событиях или действиях, создающих угрозу** государственной, военной, экономической или экологической безопасности РФ.



В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого преступления, а также при наличии данных о событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности РФ, на основании мотивированного постановления одного из руководителей органа, осуществляющего ОРД, допускается проведение ОРМ, с обязательным уведомлением суда (судьи) в течение 24 часов.

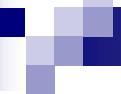
В течение 48 часов с момента начала проведения ОРМ орган, его осуществляющий, обязан получить судебное решение о проведении такого ОРМ либо прекратить его проведение.



Прослушивание телефонных и иных переговоров

допускается только в отношении лиц, подозреваемых или обвиняемых в совершении тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях.

Фонограммы, полученные в результате прослушивания телефонных и иных переговоров, хранятся в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами.



В случае возбуждения уголовного дела в отношении лица, телефонные и иные переговоры которого прослушиваются, фонограмма и бумажный носитель записи переговоров передаются следователю для приобщения к уголовному делу в качестве вещественных доказательств.

Дальнейший порядок их использования определяется уголовно-процессуальным законодательством РФ.

В случае угрозы жизни, здоровью, собственности отдельных лиц с их согласия в письменной форме разрешается прослушивание переговоров, ведущихся с их телефонов, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего суда в течение 48 часов.

Исключение составляет только радиосвязь, осуществляемая с помощью радиостанций, для прослушивания которой судебного решения не требуется.

Срок действия вынесенного судьей постановления исчисляется в сутках со дня его вынесения и не может превышать шести месяцев.

Право осуществлять оперативно-розыскную деятельность (статья 13) на территории РФ предоставлено:

- 1. Органам внутренних дел РФ;**
- 2. ФСБ;**
- 3.Федеральным органам государственной охраны:
Главному управлению охраны РФ и
Службе безопасности Президента РФ;**
- 4.Таможенным органам РФ.**
- 5.Службе внешней разведки РФ.**
- 6. Федеральной службы исполнения наказаний.**
- 7.Органов по контролю за оборотом наркотических средств и психотропных веществ.**

Контроль за ОРД

Контроль за ОРД осуществляют Президент, Федеральное Собрание и Правительство РФ (ст. 20).

В соответствии со статьей 21 предусмотрен **прокурорский надзор** за ОРД. Прокурорский надзор осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

Предусмотрен также **ведомственный контроль** (ст. 22). Руководители органов, осуществляющих ОРД, несут персональную ответственность за законность при организации и проведении ОРМ.

Отдельным законом регулируется деятельность ФСБ.
Это закон “Об органах ФСБ в РФ” от 3.04.95г. №40-ФЗ.

На ФСБ возложены функции по организации системы защиты государственных секретов и ее методического обеспечения, а также оказание содействия негосударственным учреждениям, организациям и предприятиям в вопросах защиты коммерческой тайны и другой приоритетной информации.

Это дает основания всем заинтересованным субъектам соответствующих правовых отношений обращаться к органам ФСБ за содействием в обеспечении защиты коммерческой информации. Такое содействие может выражаться в консультировании, оказании технической и организационной помощи.



В ст. 6 закона говорится о соблюдении прав и свобод человека при деятельности органов ФСБ.

Полученные в процессе деятельности органов ФСБ сведения о частной жизни, не могут сообщаться органами ФСБ без добровольного согласия гражданина.

В случае нарушения сотрудниками органов ФСБ прав и свобод человека и гражданина руководитель ФСБ, прокурор или судья обязаны принять меры по восстановлению этих прав и свобод, возмещению причиненного ущерба и привлечению виновных к ответственности, предусмотренной законодательством.



Должностные лица ФСБ, допустившие злоупотребление властью или превышение служебных полномочий, несут ответственность, предусмотренную законодательством РФ.

Для осуществления своей деятельности **органы ФСБ могут без лицензирования разрабатывать, создавать и эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации, включая средства криптографической защиты** (ст. 20).

Контроль за деятельностью органов ФСБ

**осуществляют Президент, Федеральное Собрание и
Правительство РФ (ст. 23).**

Надзор за исполнением органами ФСБ законов РФ

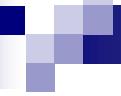
**осуществляют Генеральный прокурор РФ и
уполномоченные им прокуроры (ст. 24).**

Имеются и другие правовые акты, регламентирующие деятельность этих органов так в “Положении о Федеральной государственной службе” сказано, что государственный служащий обязан сохранять ГТ и иную охраняемую законом РФ тайну, в том числе и после прекращения государственной службы.

7.3. Защита коммерческой информации от неправомерных действий контролирующих и правоохранительных органов

Законодательной базой, регулирующей правовые отношения с контролирующими и правоохранительными органами, являются следующие документы:

1. Закон РФ “О защите конкуренции” 26 июля 2006 года № 135-ФЗ.
2. Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”, №948-1 от 22 марта 1991 г.
(В ред.от 26.07.2006 № 135-ФЗ.)
3. Закон РФ “О полиции”, №3 ФЗ от 07 февраля 2011 г.
4. Закона РФ “О санитарно-эпидемиологическом благополучии населения”, от 30.03.99 №52-ФЗ (Ред. 8.11.2007 г. N 258-ФЗ)
5. Закон РФ “О банках и банковской деятельности”, от 3.02.96г. №17-ФЗ.
(Ред. от 29.12.2006 № 246-ФЗ)



Одной из форм недобросовестной конкуренции **является**, согласно закона “О защите конкуренции”, **получение, использование, разглашение научно-технической, производственной или торговой информации, в том числе КТ без согласия ее законного владельца (ст.14).**

К числу контролирующих органов **относится федеральный антимонопольный орган, который имеет свои территориальные управлении.**

В настоящее время функции федерального антимонопольного органа осуществляет Федеральная антимонопольная служба (ФАС). Положение о Федеральной антимонопольной службе принято Правительством России 29 июля 2004 г.

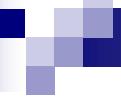
Антимонопольный орган располагает для выполнения возложенных функций значительными полномочиями (беспрепятственный доступ в органы управления, на предприятия, право на ознакомление со всеми необходимыми документами и др.).

Одна из его обязанностей - соблюдение КТ.

Сведения о ней, полученные в порядке выполнения возложенных обязанностей, не подлежат разглашению.

В случае разглашения сотрудниками ФАС сведений, составляющих КТ, причиненные убытки подлежат возмещению в соответствии с гражданским законодательством.

Информация, составляющая коммерческую, служебную, иную охраняемую законом тайну, представляется в антимонопольный орган в соответствии с требованиями, установленными федеральными законами и не подлежит разглашению, за исключением случаев, установленных федеральными законами.

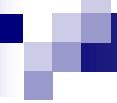


За разглашение информации, составляющей коммерческую, служебную, иную охраняемую законом тайну, работники антимонопольного органа несут гражданско-правовую, административную и уголовную ответственность.

Вред, причиненный физическому или юридическому лицу в результате разглашения антимонопольным органом либо его должностными лицами информации, составляющей коммерческую, служебную, иную охраняемую законом тайну, подлежит возмещению за счет казны РФ (ст. 26).

Вопросы, связанные с полномочиями органов МВД
отражены в Закон РФ «О полиции» от 7 февраля 2011 г.

Законом определено (ст. 11), что **сотрудники полиция
вправе беспрепятственно входить в помещения,**
занимаемые предприятиями, учреждениями,
организациями, независимо от подчиненности и форм
собственности, **только при наличии данных о**
влекущем уголовную или административную
ответственность нарушении законодательства, и
производить осмотр в присутствии не менее двух
понятых и представителя юридического лица.



Поэтому собственник или его представитель вправе потребовать от работника полиции сведений, объясняющих необходимость вхождения на предприятие (или иной объект, например, факт возбуждения уголовного дела либо получения сведений при расследовании иного дела, его номер и орган, осуществляющий расследование).

Осмотр производственных, складских, торговых и иных служебных помещений, транспортных средств, других мест хранения и использования имущества производится только с участием собственника либо его представителей или уполномоченных им лиц.

Контроль за деятельностью полиции (ст. 37),
осуществляют Президент, Федеральное Собрание,
Правительство РФ и органы законодательной и
исполнительной власти субъектов РФ.

Надзор за законностью деятельности полиции
осуществляют Генеральный прокурор РФ и
подчиненные ему прокуроры (ст. 38).

Вред, причиненный гражданам, предприятиям,
учреждениям и организациям сотрудником полиции,
подлежит возмещению в порядке, предусмотренном
гражданским законодательством (ст.40).

Значительными полномочиями по проверке соблюдения на предприятиях санитарных правил, норм и гигиенических нормативов обладают должностные лица и специалисты Государственной санитарно-эпидемиологической службы РФ в соответствии с законом “О санитарно-эпидемиологическом благополучии населения”, 1991г. (ред. 31 декабря 2005).

Должностные лица, осуществляющие государственный санитарно-эпидемиологический надзор, **обязаны соблюдать государственную, врачебную и иную охраняемую законом тайну** в отношении информации, ставшей им известной при выполнении своих служебных обязанностей, **и несут ответственность** за ненадлежащее исполнение своих служебных обязанностей.

Закона РФ “О банках и банковской деятельности” устанавливает, что кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов.

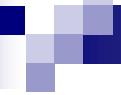
Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и их работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном законом (ст. 26).

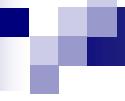
Санкции за нарушения прав владельца информации контролирующими и правоохранительными органами **представлены в УК РФ ст. 183. «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».**

Вопросы по теме 7

- 1. Каким законом регулируется деятельность органов, занимающихся оперативно-розыскной деятельностью?**
- 2. Что в соответствии с законом производится с собранными материалами в отношении лиц, виновность которых не доказано?**
- 3. Допускается ли проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина?**
- 4. Каким законом регулируется деятельность ФСБ по соблюдению прав и свобод граждан?**
- 5. Публикуются ли в открытой печати сведения об организации и тактики проведения оперативно-розыскных мероприятий?**



6. Куда следует обратиться юридическим и физическим лицам для защиты от неправомерных действий контролирующих органов?
7. Кем осуществляется контроль и надзор за оперативно-розыскной деятельностью?
8. Каким законом определены организационно-правовые основы пресечения недобросовестной конкуренции?
9. Каким законом регулируется деятельность банков по защите тайна вкладчиков?
10. Каким законом регулируется деятельность санитарно-эпидемиологических служб РФ по сохранности КТ проверяемых предприятий?
11. Могут ли органы ФСБ без лицензирования разрабатывать, создавать и эксплуатировать средства защиты информации, включая криптографические?



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

К.Т.Н.

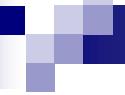
Струков Владимир Ильич

8. Правовая защита конфиденциальной информации

8.1. Сведения конфиденциального характера

В действующем законодательстве РФ упоминается более 40 видов тайн
(банковская, налоговая, коммерческая, профессиональная и т.д.),
а с учетом законодательства Союза Россия – Беларусь таких тайн более 50.

В законе «Об информации...» нет термина «конфиденциальная информация», но дается определение понятия «конфиденциальность информации».



Указом Президента Российской Федерации № 188 от 06.03.97г. (ред. от 23.09.2005 №1111) был утвержден **Перечень сведений «конфиденциального характера»**, где указаны **шесть видов такой информации:**

- ▶ **персональные данные;**
- ▶ **тайна следствия и судопроизводства;**
- ▶ **служебная тайна;**
- ▶ **профессиональная тайна;**
- ▶ **коммерческая тайна;**
- ▶ **сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о них.**

Однако, данный перечень может быть утвержден только законом в соответствии с нормами международного права и Конституции РФ.

Отсутствие в законах четких определений видов информации с ограниченным доступом (за исключением государственной тайны) приводит к противоречиям между данным указом и существующими законодательными актами, что затрудняет их исполнение.

Например, в действующих кодексах есть такие понятия как личная, семейная тайны и неприкосновенность частной жизни, а в других законах - персональные данные.

В действующих законах нет понятия «тайна следствия и судопроизводства», но есть понятия «данные предварительного расследования», «данные предварительного следствия», «тайна совещания судей», «тайна совещания присяжных заседателей».

В законах не дается понятия служебной тайны и в то же время применяется понятие «служебная информация». Соотношение между ними не установлено, а в указе вводится категория только служебной тайны.

Грифы конфиденциальности

Для обозначения грифа конфиденциальности используются международные и национальные нормативные документы. Причем требования российского законодательства отличаются от международных стандартов.

Так в соответствии со международным стандартом ISO 17799 «Безопасность информационных систем» используются следующие обозначения:

ОТ - открытая информация;

КИ - конфиденциальная информация;

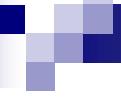
СКИ - строго конфиденциальная информация.

В российском законодательстве используются следующие термины:

ОТ - открытая информация;

ДВИ – для внутреннего использования;

КИ - конфиденциальная информация.



Из указанных видов информации в
действующем законодательстве наименее
разработанными являются

профессиональная тайна

и

служебная тайна

8.2. Нормативно-правовое регулирование профессиональной тайны

В современном законодательстве РФ не принят закон «О профессиональной тайне» и нет чёткого определения профессиональной тайны.

Профессиональная тайна –

защищаемая по закону
информация, доверенная лицу
в силу исполнения им своих
профессиональных обязанностей,
не связанных с государственной
и муниципальной службой и не
являющаяся государственной
или коммерческой тайной,

распространение которой может нанести ущерб интересам
лица, доверившего эти сведения.

В соответствии с данным определением выделяются
следующие объекты профессиональной тайны:

Врачебная тайна - информация содержащая:

- результаты обследования лица, вступающего в брак;
- сведения о факте обращения за медицинской помощью, иные сведения о состоянии здоровья.

Тайна связи - тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Нотариальная тайна – сведения, доверенные нотариусу в связи с совершением нотариальных действий.

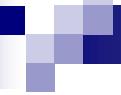
Адвокатская тайна – сведения, сообщенные адвокату гражданином в связи с оказанием юридической помощи.

Тайна усыновления – сведения об усыновлении ребенка усыновителем.

Тайна страхования - сведения о страхователе, застрахованном лице и выгодоприобретателе.

Тайна исповеди - сведения, доверенные священнослужителю гражданином на исповеди.

Журналистская тайна – сведения, сообщенные журналисту.



Правовые документы о профессиональной тайне:

1. Законы РФ :

ГК РФ (ст. 964);

УК РФ (ст.155);

ГПК РСФСР (ст.9);

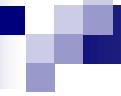
УПК РСФСР (ст.51);

Семейный кодекс РФ (ст.15, 139);

ФЗ «О связи» (ст.32) от 16.02.1995г. ;

«Основы законодательства РФ об охране здоровья граждан» от 22.07.1993г. (ст.30,31,35,49,61);

ФЗ от 02.07.1992г. «О психиатрической помощи и гарантиях прав граждан при ее оказании» (ст.9,46);

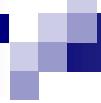


ФЗ «**О религиозных объединениях**» от 25.07.2002г. №112 ;
закон РСФСР «**Об утверждении положения об адвокатуре РСФСР**» от 20.11.1980г. (ст. 16);
«Основы законодательства РФ о нотариате» от 10.02.1993г. (ст.5, 14,16,17,28,34);
ФЗ от 22.12.1992г. «**О трансплантации органов и (или) тканей человека**» (ст.14);
ФЗ «**О социальном обслуживании граждан пожилого возраста и инвалидов**» от 17.05.1995г. №122 – ФЗ (ст.11);
ФЗ "О средствах массовой информации" от 27 декабря 1991 г. №2124-1 (ст. 41).

2. Подзаконные акты

Постановления Правительства РФ:

- №352 от 28.05.1992г. (в ред. Постановления №792 от 02.07.1997г.) «О заключении межправительственных соглашений об избежании двойного налогообложения доходов и имущества» (ст.23);
- №1235 от 26.09.1997г. «Об утверждении правил оказания услуг телефонной связи» (п.8);
- №1239 от 26.09.1997г. «Об утверждении правил оказания услуг почтовой связи (п.132,140);
- №1017 от 13.10.1995г.;
- №221 от 28.02.1996г. «Об утверждении правил обязательного медицинского освидетельствования на выявление ВИЧ-инфекции» и др.



3. Судебная практика:

постановление Конституционного суда РФ №8-П от 27.03.1996г. (в части профессиональной тайны адвоката);

постановление Пленума Верховного суда РФ №10 от 20.12.1994г. «Некоторые вопросы применения законодательства о компенсации морального вреда» и д.р.

4. Международные договоры и соглашения-

более 30 двусторонних соглашений об избежании двойного налогообложения доходов и имущества и др.

В законодательстве не предусматривается сегодня возможность доступа к профессиональной тайне, со стороны государственных органов – только в двух случаях: в отношении адвокатской тайны и тайны исповеди.

В УК РФ прямо предусматривается уголовная ответственность лишь в случае разглашения двух видов профессиональной тайны – тайны усыновления (ст. 155 УК РФ) и тайны связи (ст. 138 УК РФ).

Нормативно-правовое регулирование профессиональной тайны

Врачебная тайна	Тайна связи	Нотариальная тайна
Адвокатская тайна	Тайна усыновления	Тайна страхования
Тайна исповеди	Журналистская тайна	

Законы РФ:

"Основы законодательства РФ о нотариате"

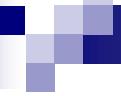
"О СМИ"

"Семейный кодекс РФ" - (Тайна усыновления - уголовная ответственность за разглашение)

"О связи" - (Тайна связи - уголовная ответственность за разглашение).

"Об утверждении положения об адвокатуре РФ" - (Нет доступа со стороны государственных органов к адвокатской тайне).

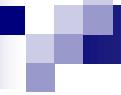
"О религиозных объединениях" - (Нет доступа со стороны государственных органов к тайне исповеди).



УК РФ Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан -

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.



2. То же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от двух до четырех месяцев.

УК РФ Статья 155. Разглашение тайны усыновления (удочерения)

Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иным лицом из корыстных или иных низменных побуждений, -

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

В предполагаемом законе «О профессиональной тайне» должны быть даны определения, например:

- **Профессиональная тайна** – это сведения полученные представителями некоторых профессий в силу исполнения ими своих профессиональных обязанностей.
- **Доверитель** – физическое или юридическое лицо, доверившее сведения другому лицу, а также его правопреемники.
- **Держатель профессиональной тайны** – юридическое или физическое лицо-специалист, которому исключительно в силу его профессиональных обязанностей доверитель представил сведения, составляющие профессиональную тайну.
- **Пользователь профессиональной тайны** – лицо, которому сведения, составляющие профессиональную тайну, стали известны на законных основаниях в связи с выполнением им своих служебных обязанностей.

И приведен перечень видов профессиональной тайны

Например, в некоторых европейских странах в Законе «О профессиональной тайне» указывается более широкий перечень профессий, попадающих в сферу его действия:

медицинские работники, адвокаты, нотариусы, управляющие делами, бухгалтера, аудиторы, служащие финансовых и кредитных организаций, поверенные, должностные лица компаний, лица, оказывающие инвестиционные услуги, биржевые маклеры, страховщики, страховые агенты, страховые брокеры, государственные официальные лица и служащие.

8.3. Нормативно-правовое регулирование служебной тайны

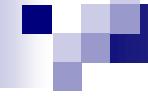
Должностная служебная тайна связана с интересами государственной службы и службы в органах местного самоуправления.

Доступ к служебным сведениям закрытого характера связан с должностным статусом лиц, которым эти сведения стали известны по службе.

Поэтому при утечки этой секретной информации страдают интересы службы (а не клиентов, как в случае профессиональной тайны).

В 2003 г. был внесен в думу законопроект «О служебной тайне» в котором рассмотрены вопросы отнесения и защиты сведений, составляющих служебную тайну.

Сведения, составляющие служебную тайну (СТ) - конфиденциальные сведения, образующиеся в процессе управленческой деятельности органа, распространение которых препятствует реализации органом предоставленных ему полномочий, либо отрицательно сказывается на их реализации, а также конфиденциальные сведения, полученные органом в соответствии с его компетенцией в установленном законодательством порядке.



Определен механизм отнесения сведений к СТ

К сведениям, которые органы государственной власти и их организации обязаны защищать в режиме служебной тайны, относятся -

поступившие от физических и юридических лиц, других органов государственной власти и организаций **сведения, доступ к которым ограничен в соответствии с федеральными законами, при наличии на документах, содержащих эти сведения или сопроводительных документах, соответствующих пометок, указывающих на их конфиденциальный характер.**

Отнесение сведений к служебной тайне осуществляется на основании перечней сведений, разрабатываемых органами государственной власти и утверждаемых их руководителями путем установления соответствия содержащихся в документе сведений перечню сведений, отнесенных к служебной тайне, действующего в данном органе государственной власти.

Определен режим служебной тайны – совокупность правовых, организационных, технических и иных мер, принимаемых уполномоченными должностными лицами органов государственной власти и организаций, обеспечивающих ограничения на распространение сведений, составляющих служебную тайну, и на доступ к этим сведениям.

Документы, содержащие сведения, составляющие служебную тайну, независимо от формы представления этих документов, должны включать помимо обязательных реквизитов, следующие:

- пометку "для служебного пользования";
- **наименование органа государственной власти, установившего ограничения на распространение сведений;**
- **регистрационный номер документа в системе делопроизводства;**
- **дату снятия ограничений на распространение сведений,** либо событие, при наступлении которого ограничения подлежат отмене;
- **наименование должности лица, подписавшего документа** его собственноручную подпись или электронную цифровую подпись, используемую в соответствии с законодательством РФ.

Обеспечение режима служебной тайны в органах и организациях осуществляется структурными подразделениями по защите служебной тайны.

Для защиты сведений, составляющих служебную тайну, должны использоваться средства защиты информации, прошедшие сертификацию.

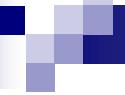
Документы, содержащие сведения, составляющие служебную тайну, не должны включаться в электронные информационные системы, имеющие подключение к сети связи общего пользования.

Обязательства работника по неразглашению СТ, могут сохраняться после прекращения трудовых отношений на срок, определенный в трудовом договоре либо отдельном соглашении, но не свыше пяти лет.

Негосударственные организации получают доступ к СТ, только в рамках гражданско-правовых отношений с заказчиком, которым является орган государственной власти или государственная организация.

Договор на выполнение работ или предоставление услуг между органом или организацией-заказчиком и негосударственной организацией-исполнителем должен включать положения, регламентирующие порядок обращения со сведениями, составляющими служебную тайну, и гражданско-правовую ответственность за разглашение указанных сведений.

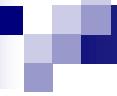
Так как закон «О служебной тайне» до сих пор не принят, применяются нормы существующей правовой базы



Определение понятия «**служебная тайна**» дано в ст.139 части первой ГК РФ, называющейся “**Служебная и коммерческая тайна**”:

-информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

Примерами противоправных действий являются: разглашение судьями тайны совещания при вынесении приговора, должностными лицами Банка России банковской тайны, работниками налоговой инспекции налоговой тайны (сведения о налогоплательщике).



Информация может считаться служебной тайной, если она:

- ▶ **отнесена федеральным законом к служебной информации** о деятельности государственных органов, доступ к которой ограничен;
- ▶ **является охраноспособной конфиденциальной информацией («чужой тайной»)** другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна);
- ▶ **не является государственной тайной** и не подпадает под перечень сведений, доступ к которым не может быть ограничен;
- ▶ **получена представителем государственного органа и органа местного самоуправления** только в силу исполнения обязанностей по службе в случаях и порядке, установленных федеральным законом.

Перечень сведений, которые не могут быть отнесены к служебной информации ограниченного доступа:

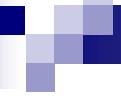
- ▶ **акты законодательства**, устанавливающие правовой статус государственных органов, организаций, граждан;
- ▶ **сведения о чрезвычайных ситуациях**, опасных природных явлениях и процессах;
- ▶ **описание структуры органа исполнительной власти**, его функций, направлений и форм деятельности, а также его адрес;
- ▶ **порядок рассмотрения и разрешения заявлений**, в том числе юридических лиц;
- ▶ **сведения об исполнении бюджета и использовании других государственных ресурсов;**
- ▶ **документы, накапливаемые в открытых фондах** библиотек и архивов, информационных системах организаций.

Основными объектами служебной тайны являются:

- **служебная информация о деятельности федеральных государственных органов**, доступ к которой ограничен федеральным законом **в целях защиты государственных интересов**: военная, тайна; тайна следствия; судебная тайна (тайна совещания судей, тайна совещания присяжных заседателей, порядок выработки и принятия решения, организация внутренней работы и т.д.);
- **охраноспособная конфиденциальная информация**, ставшая известной в силу исполнения служебных обязанностей должностным лицам государственных органов и органов местного самоуправления: коммерческая тайна, банковская тайна, профессиональная тайна, а также конфиденциальная информация о частной жизни лица.

Законодательные документы в отношении защиты служебной тайны:

1. Закон РФ от 31.07.95 №119-ФЗ “Об основах государственной службы РФ”.
2. Закон РФ от 17.01.92 №2202-1 “О прокуратуре РФ”.
3. Закон РФ от 02.12.90 №395-1 “О банках и банковской деятельности”.
4. Закон РФ от 07 февраля 2011 г. №3 ФЗ “О полиции”.
5. Закон РФ от 12.08.95г. №144-ФЗ “Об оперативно-розыскной деятельности”.
6. Закон РФ от 16.02.95 №15-ФЗ “О связи”.
7. Закон РФ от 29.07.2004г. №98-ФЗ "О коммерческой тайне".
8. Гражданский кодекс РФ от 13.06.96 №63-ФЗ.
9. Таможенный кодекс РФ утв. ВС РФ 18.06.93 №5221-1.



Ответственность за разглашение «**служебной тайны**» дана в ст.139 части первой ГК РФ “**Служебная и коммерческая тайна**”:

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки.

Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Пример защиты налоговой тайны.

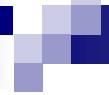
Понятие налоговой тайны введено Налоговым кодексом РФ. Согласно ст.102 НК РФ это сведения о налогоплательщике, полученные налоговой инспекцией или таможенным органом при налоговом контроле.

Режим хранения сведений, составляющих НТ, и доступа к ним устанавливается МНС РФ.

Часть 4 ст.102 НК РФ определяет два вида нарушений в отношении НТ:

- разглашение НТ;**
- утрата документов, содержащих налоговую тайну организации.**

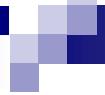
За эти нарушения виновные привлекаются к ответственности.



За утрату документов сотрудники налоговых органов несут дисциплинарную ответственность.

Если же при этом по их вине разглашена не только налоговая, но и **коммерческая** или банковская тайна, то **может наступить уголовная ответственность по ст.183 УК РФ.**

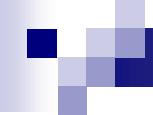
Утрата документов и предметов, содержащих секретные сведения, не повлекшая за собой тяжких последствий – состава преступления не образует.



К материальным носителям сведений содержащим служебную, ГТ или КТ относятся: бумага, магнитная лента, физические поля, фото- и кинопленка, диски, лазерные диски и др. носители.

Материальные носители секретных сведений имеют **регистрационный номер, гриф секретности, установленный порядок хранения, выдачи, размножения и уничтожения.**

Они могут быть официальными или неофициальными (черновики, наброски).



Коммерческая тайна – связанная с производственной, технической, технологической информацией, управлением финансовой и другой деятельностью предприятия, разглашение (передача, утечка) которой может нанести ущерб его интересам.

Персональные данные – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.

Служебная информация – служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами.

Профессиональная тайна – информация, передаваемая по линиям связи.

Режим коммерческой тайны считается установленным, если обладатель КТ принял меры (в соответствии с законом «О коммерческой тайне»):

- определен перечень информации**, составляющей КТ, и довел их до сведения работников **под распись**;
- ограничил свободный доступ** к информации, составляющей коммерческую тайну;
- организовал **договорное регулирование отношений** с работниками по вопросам условий передачи и использования информации, составляющей КТ;
- нанес на материальные носители информации, составляющей КТ, и (или) сопроводительные документы **гриф «Коммерческая тайна»**.
- ознакомил **под распись** работника с установленным на предприятии **режимом КТ**.

В статье 139 ГК РФ предусмотрено, что **обладатель КТ вправе требовать возмещения убытков в следующих 4-х случаях:**

- от лиц, незаконными методами получивших информацию, составляющую КТ, например, путем похищения;
- от работника, разгласившего КТ вопреки трудовому договору. *В этом случае работник получает информацию, содержащую КТ, на законных основаниях, например в силу занимаемой должности, а ответственность наступает за незаконное ее разглашение.* При этом обязательным является наличие условия о неразглашении КТ в трудовом договоре. Работодатель обязан ознакомить работника под роспись с перечнем сведений, содержащих КТ;

- от контрагента, разгласившего КТ вопреки гражданско-правовому договору. *Под контрагентом следует понимать любое лицо, с которым у обладателя информации заключено соглашение о ее неразглашении. В этом соглашении обязательно должно быть указано какая именно информация является коммерческой тайной;*
- в результате неправомерного разглашения КТ должностными лицами государственных органов, получившими ее на законных основаниях.

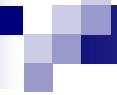
За исключением четырех вышеперечисленных, случаев нарушения коммерческой тайны не происходит, соответственно права на возмещение ущерба не появляется.

Для взыскания убытков лицу, требующему их возмещения, придется доказать в суде следующие факты (ст. 53 АПК):

во-первых, что имело место незаконное получение или разглашение коммерческой тайны;

во-вторых, предоставить суду расчет понесенных убытков. При этом стоимость информации, составляющей КТ, определить более чем сложно. Можно поступить следующим образом. Заключить с лицом, которое посвящено в секреты фирмы, гражданско-правовой договор, в соответствии с которым лицо обязуется не разглашать определенную информацию.

Ответственность в случае разглашения информации устанавливается в виде штрафной неустойки, то есть фиксированной суммы. При этом предприятие не обязано доказывать причинение ему убытков (п. 1 ст. 330 ГК РФ);



в-третьих, наличие причинной связи между понесенными убытками и совершенным правонарушением.

Только доказав все выше перечисленные факты и представив обоснованный расчет причиненных недобросовестным конкурентом убытков потерпевшее лицо вправе будет рассчитывать на положительное для себя решение суда.

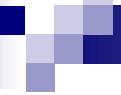
Конфиденциальная информация, как любой товар, продается и покупается. И что бы ее получить порой бывает достаточно заплатить определенную сумму человеку, имеющему к ней законный доступ.

Среди таких действий может быть **разглашение** этим лицом информации, составляющую КТ организации, раскрытие **производственных секретов**, дающее стороне, подкупившей соответствующего служащего конкурирующего предприятия, незаслуженное **преимущество в хозяйственной деятельности**.

В российском законодательстве предусмотрена ответственность за **коммерческий подкуп**.

УК РФ Статья 204. Коммерческий подкуп

1. Незаконная передача лицу, выполняющему управленческие функции в коммерческой или иной организации, денег, ценных бумаг, иного имущества, а равно незаконное оказание ему услуг имущественного характера за совершение действий (бездействия) в интересах дающего в связи с занимаемым этим лицом служебным положением - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет, либо ограничением свободы на срок до двух лет, либо лишением свободы на срок до трех лет.



УК РФ Статья 204. Коммерческий подкуп

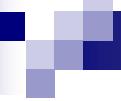
2. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой, - наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо ограничением свободы на срок до трех лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до четырех лет.

УК РФ Статья 204. Коммерческий подкуп

3. Незаконное получение лицом, выполняющим управленческие функции в коммерческой или иной организации, денег, ценных бумаг, иного имущества, а равно незаконное пользование услугами имущественного характера за совершение действий (бездействия) в интересах дающего в связи с занимаемым этим лицом служебным положением - наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

УК РФ Статья 204. Коммерческий подкуп

4. Деяния, предусмотренные частью третьей настоящей статьи, если они:
 - а) совершены группой лиц по предварительному сговору или организованной группой;
 - б) сопряжены с вымогательством предмета подкупа, - наказываются лишением свободы на срок от семи до двенадцати лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.



УК РФ Статья 204. Коммерческий подкуп

Примечание.

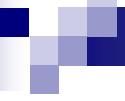
Лицо, совершившее деяния, предусмотренные частями первой или второй настоящей статьи, освобождается от уголовной ответственности, если в отношении его имело место вымогательство или если это лицо добровольно сообщило о подкупе органу, имеющему право возбудить уголовное дело.

УК РФ Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов

1. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами, - наказываются лишением свободы на срок от двух до шести лет со штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.
2. Те же деяния, совершенные организованной группой, - наказываются лишением свободы на срок от четырех до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового.

Контрольные вопросы

- 1. Нормативно-правовое регулирование профессиональной тайны в РФ.**
- 2. Признаки и объекты профессиональной тайны.**
- 3. Какие сведения относятся к служебной тайне?**
- 4. На каких правовых актах основана защита служебной и коммерческой информации на предприятии?**
- 5. Чем отличается служебная тайна от профессиональной?**
- 6. Внутренние нормативные документы, которые используются для правовой защиты служебной и КТ.**
- 7. Какой закон регулирует отношения, связанные с отнесением информации к коммерческой тайне?**
- 8. В каких случаях обладатель КТ вправе требовать возмещения убытков?**



Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

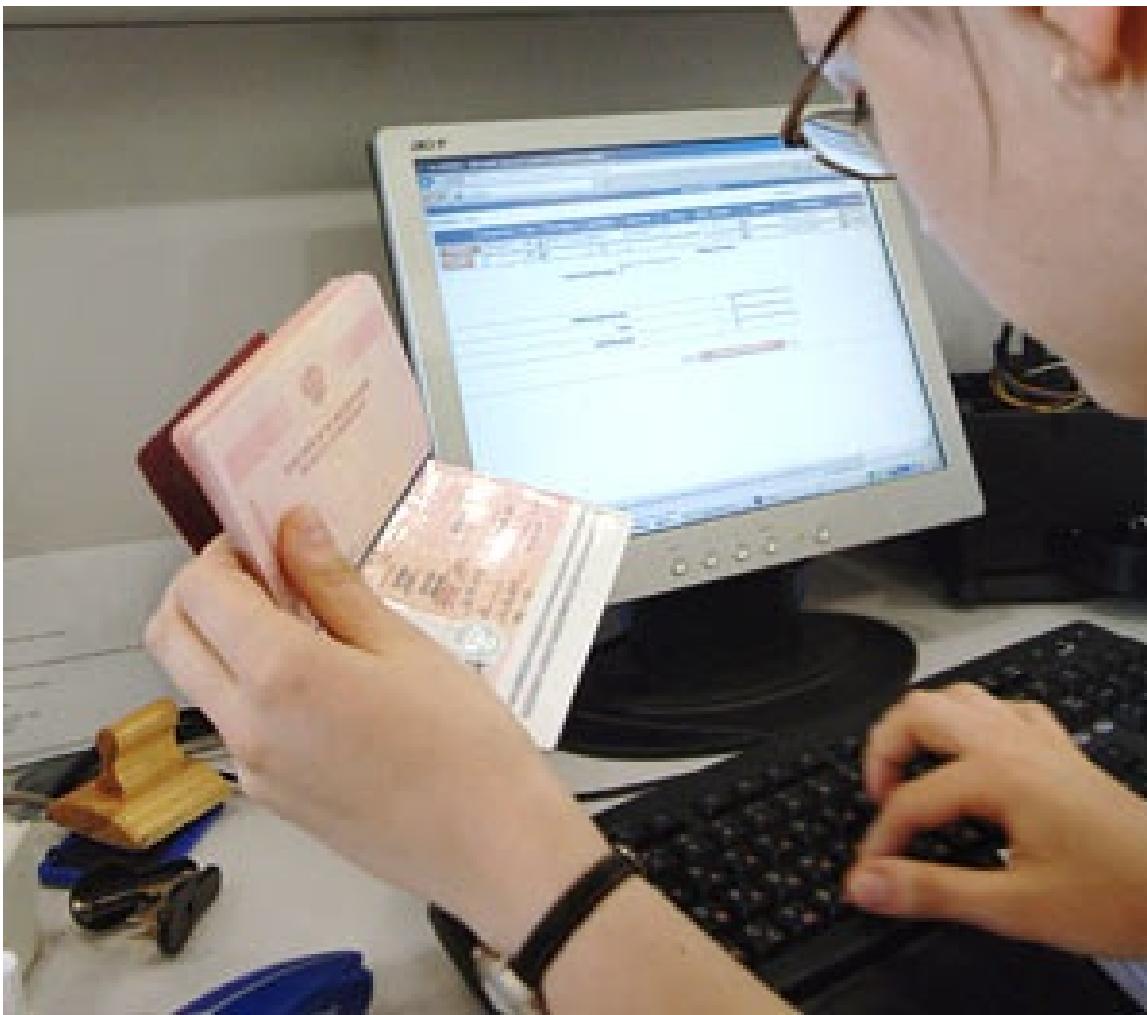
К.Т.Н.

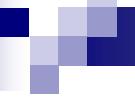
Струков Владимир Ильич

Вопросы к разделу 8.1

- 1. Нормативно-правовое регулирование профессиональной тайны в РФ.**
- 2. Признаки и объекты профессиональной тайны.**
- 3. Какие сведения относятся к служебной тайне?**
- 4. На каких правовых актах основана защита служебной и коммерческой информации на предприятии?**
- 5. Чем отличается служебная тайна от профессиональной?**
- 6. Внутренние нормативные документы, которые используются для правовой защиты служебной и КТ.**
- 7. Какой закон регулирует отношения, связанные с отнесением информации к коммерческой тайне?**
- 8. В каких случаях обладатель КТ вправе требовать возмещения убытков?**

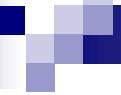
8.4. Правовое обеспечение защиты персональных данных (ПД)





Необходимость принятия мер по защите ПД было вызвано двумя факторами:

- 1. Высокий уровень хищения этой информации инсайдерами.**
- 2. Наличие несоответствия правовых норм защиты ПД в России и в Евросоюзе, мешающего развитию торговли с европейскими странами.**



Согласно данным компании Perimetrix, опубликованным в интернет-СМИ утечки данных определяется внутренними угрозами информационной безопасности :

На первом месте по количеству случаев, находятся инсайдеры (76%).

На втором месте – сотрудники, которые теряют важные данные из-за халатности, невнимательности или незнания основных правил безопасности (67%).

Всего 5% организаций в 2007 году не пострадали от утечек.

К инсайдерам относят:

- сотрудников, сознательно работающих на конкурентов (нанятых или предварительно трудоустроенных ими);**
- сотрудников, прямо или косвенно связанных с криминальными структурами;**
- просто недобросовестных сотрудников, ставящих свои интересы заведомо выше интересов фирмы;**
- сотрудников, обиженных на начальство и по этой причине скрытно вредящих, не получая от этого какой-либо выгоды.**

Чаще всего инсайдеров интересуют персональные данные (из-за большого спроса на них).

За персональными данными по «популярности» в среде инсайдеров следуют детали конкретных сделок (47%), финансовые отчеты (38%), интеллектуальная собственность компании (25%), бизнес-планы (19%) и прочие информационные ресурсы (14%).

Каналы утечки данных распределились так:

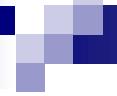
1. Мобильные накопители – 74%
2. Электронная почта – 58%
3. Интернет-пейджеры (IM) – 17%
4. Интернет (web-почта, форумы, блоги) – 26%
5. Принтеры – 18%
6. Фото-видео-устройства – 2%
7. Другие – 5%

Сумма более 100% т.к. ни один инсайдер не пользуется единственным каналом передачи данных.

Европейская Конвенции 1981 года «О защите личности в связи с автоматической обработкой персональных данных», определила основные принципы защиты ПД в европейских странах.

Согласно Директиве 95/46/ЕС Евросоюза ПД могут передаваться только в страны, обеспечивающие такой же уровень защиты, как и в Европе.

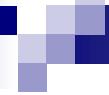
Несоответствие правовых норм защиты ПД в российском законодательстве требованиям указанной Конвенции, к которой присоединилась Россия (конвенция ратифицирована ФЗ от 19 декабря 2005 года N 160-ФЗ), тормозило обмен сведениями с европейскими государствами и компаниями, делая невозможными многие коммерчески перспективные проекты.



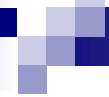
Закон РФ № 152-ФЗ «О персональных данных» устранил указанные препятствия, во многом повторив основные положения европейского законодательства в данной сфере.

Конвенция и последовавшие за ней Директивы Евросоюза сформулировали следующие задачи, которые должно регулировать национальное законодательство в отношении ПД:

-защита ПД от НСД к ним со стороны других лиц, в том числе представителей государственных органов и служб, не имеющих на то необходимых полномочий;



- обеспечение сохранности, целостности и достоверности данных в процессе работы с ними, в том числе при передаче по каналам связи;
- обеспечение надлежащего правового режима этих данных при работе с ними для различных категорий ПД;



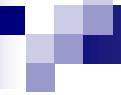
- обеспечение контроля над использованием ПД со стороны самого гражданина;
- создание специальной независимой структуры, обеспечивающей эффективный контроль за соблюдением прав гражданина на защиту его ПД (например, создание должности Уполномоченного по защите ПД). Таковым в настоящее время органом является Роскомнадзор.

Проблемы защиты ПД

Для выполнения требований закона, существенно изменяется работа с документами, содержащими ПД.

1. Во всех организациях появляется новый, объемный пакет документов. Это документы, связанные с получением согласия физических лиц на обработку их ПД, с регистрацией баз данных в уполномоченном органе, с документированием всех операций с ПД и т.д.
2. Возникает необходимость выделения содержащих ПД документов и информации; их особой маркировки как на бумажных, так и на электронных носителях; ведения отдельного учета и отслеживания доступа к ним.

3. Устанавливается норматив сроков хранения документов и информации и максимальный срок хранения, который необходимо соблюдать и отслеживать.
4. При работе с ПД необходимо заранее продумать и зафиксировать в нормативных документах все, что связано с их обработкой. В противном случае организация может быть привлечена к ответственности в том числе по искам от самих субъектов персональных данных.
5. Законом вводятся жесткие сроки исполнения всех обращений граждан, связанных с обработкой ПД.

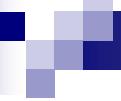


Участники правовых отношений

Закон распространяется на всех участников
(государственные, юридические и физические лица).

В соответствии со статьей 1 закона это:

- федеральные органы государственной власти,
- органы государственной власти субъектов РФ,
- иные государственные органы,
- органы местного самоуправления,
- не входящие в систему органов местного самоуправления муниципальные органы,
- юридические лица,
- физические лица.

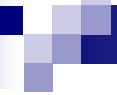


Область применения

Законом регулируются отношения, связанные с обработкой ПД при использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с ПД с использованием средств автоматизации.

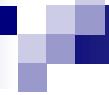
Предусмотрены следующие способы обработки ПД (ст. 3):

- сбор**;
- систематизация**;
- накопление**;
- хранение**;
- уточнение** (обновление, изменение);
- использование** — действия (операции) с ПД, совершаемые оператором в определенных целях;
- распространение** (в том числе передача) — действия, направленные на передачу ПД определенному кругу лиц;
- обезличивание** — действия, в результате которых невозможно определить принадлежность ПД конкретному субъекту;
- блокирование** — временное прекращение сбора, систематизации, накопления, использования, распространения ПД;
- уничтожение** — действия, в результате которых невозможно восстановить содержание ПД в информационной системе или в результате которых уничтожаются материальные носители ПД.



В законе предусмотрены только четыре исключения, действие закона не распространяется на отношения, возникающие:

- при обработке персональных данных для личных и семейных нужд;**
- при обработке персональных данных в документах Архивного фонда РФ;**
- при обработке персональных данных для включения их в Единый государственный реестр индивидуальных предпринимателей (ЕГРИП);**
- при обработке персональных данных, отнесенных к государственной тайне.**



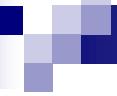
Правила обработки и обеспечения конфиденциальности ПД, собственных работников и сторонних физических лиц, персональные данные которых обрабатываются в организации, установлены:

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в ред. ФЗ от 25.07.2011 №261).

Главой 14 Трудового Кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ.

Постановлениями Правительства РФ от 17 ноября 2007 г. № 781 и от 15 сентября 2008 г. № 687.

Нормативными документами ФСБ и ФСТЭК.

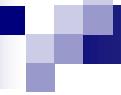


Персональными данными гражданина, подлежащим защите, признается любая информация, относящаяся к физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Безопасность ПД достигается путем исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий.

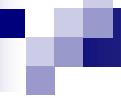
Обмен персональными данными при их обработке в информационных системах осуществляется по защищенным каналам связи.

Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях **должны** обеспечивать сохранность носителей и средств защиты информации, а также **исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц**.



При обработке персональных данных в информационной системе должно быть обеспечено:

- предотвращение НСД к данным или передачи их лицам, не имеющим права доступа;**
- своевременное обнаружение фактов НСД;**
- недопущение воздействия средства обработки данных, в результате которого они могут быть нарушено их функционирование;**
- возможность незамедлительного восстановления данных, измененных или уничтоженных при НСД;**
- постоянный контроль за обеспечением уровня защищенности ПД.**



Обработка ПД, осуществляемая без использования средств автоматизации.

Обработка ПД, содержащихся в информационной системе считается осуществленной без использования средств автоматизации, если такие действия с ПД, как использование, уточнение, распространение, уничтожение ПД в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

При этом

Обработка ПД должна осуществляться таким образом, чтобы для каждой категории ПД можно было определить места хранения ПД (материальных носителей) и установить перечень лиц, осуществляющих обработку ПД либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение ПД (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ.

Невыполнение требований указанных правовых актов по вопросам обработки ПД, может привести к

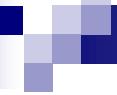
- ▶ конфликту с государственными органами, осуществляющими контроль и надзор в данной сфере деятельности (Роскомнадзор, ФСБ России, ФСТЭК России),
- ▶ привлечении организации и (или) ее руководителя к административной или иным видам ответственности.

Возможны также гражданские иски к организации, принудительное приостановление или прекращение обработки ПД в организации, приостановление действия или аннулирование лицензий.

Порядок проведения классификации информационных систем ПД

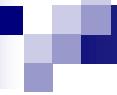
При проведении классификации информационной системы (ИС) учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных - Хпд;
- объем обрабатываемых персональных данных (количество субъектов, ПД которых обрабатываются в информационной системе) - Хнпд;
- заданные оператором характеристики безопасности ПД, обрабатываемых в информационной системе.



При проведении классификации информационной системы учитываются следующие исходные данные:

- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;
- режим обработки ПД;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.



Положением определяются следующие категории обрабатываемых в информационной системе ПД (Хпд):

категория 1 - ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

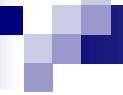
категория 2 - ПД, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1;

категория 3 - ПД, позволяющие идентифицировать субъекта персональных данных;

категория 4 - обезличенные и (или) общедоступные ПД.

ХПД может принимать следующие значения:

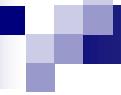
- 1 - в информационной системе одновременно обрабатываются ПД более чем 100000 субъектов персональных данных или ПД субъектов персональных данных в пределах субъекта РФ или РФ в целом;**
- 2 - в информационной системе одновременно обрабатываются ПД от 1000 до 100000 субъектов персональных данных или персональные данные субъектов ПД, работающих в отрасли экономики РФ, в органе государственной власти, проживающих в пределах муниципального образования;**
- 3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов ПД в пределах конкретной организации.**



По заданным оператором характеристикам безопасности ПД, обрабатываемых в ИС, информационные системы подразделяются на типовые и специальные информационные системы.

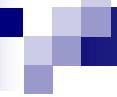
Типовые информационные системы - ИС, в которых требуется обеспечение только конфиденциальности ПД.

Специальные информационные системы - ИС, в которых вне зависимости от необходимости обеспечения конфиденциальности ПД требуется обеспечить хотя бы одну из характеристик безопасности ПД, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).



К специальным ИС должны быть отнесены:

- ИС, в которых обрабатываются ПД, касающиеся состояния здоровья субъектов персональных данных;**
- ИС, в которых предусмотрено принятие на основании исключительно автоматизированной обработки ПД решений, порождающих юридические последствия в отношении субъекта персональных данных или затрагивающих его права и законные интересы.**



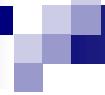
По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПД;

класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к негативным последствиям для субъектов ПД;

класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПД;

класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности ПД, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПД.



Класс типовой ИС
определяется в соответствии с таблицей.

Xнпд Xпд	3	2	1
категория 4	K4	K4	K4
категория 3	K3	K3	K2
категория 2	K3	K2	K1
категория 1	K1	K1	K1

Дополнения, связанные с принятием новых правовых актов:

- Постановление Правительства №1119 от 01.11.2012 г.
- Приказ ФСТЭК 21 от 18.02.2013 г.

Постановлением Правительства №1119

1. Даны уточнения определения ИСПДн в зависимости от категорий ПД.
2. Установлены 4 уровня защищенности ПД при их обработке в информационных системах.

Приказом ФСТЭК 21 от 18.02.2013

"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

установлен состав и содержание организационных и технических мер по защите ПД при их обработке в информационных системах персональных данных для каждого из уровней защищенности ПД в соответствии с Требованиями установленными Постановлением Правительства №1119 от 01.11.2012 г.

В отношении безопасности персональных данных различают угрозы трех типов:

- «Угрозы 1 типа..., связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении
- Угрозы 2 типа..., связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении
- Угрозы 3 типа..., не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении



Уровни защищенности ПДн в соответствии с ПП РФ от 01.11.2012 № 1119

Уровень защищенности	Тип угрозы	Категория обрабатываемых ПДн	Количество обрабатываемых данных	Требования по защите (Постановление № 1119)
1	1 типа	специальные категории	не установлено	подп. «а» п. 9
		биометрические	не установлено	подп. «а» п. 9
		иные категории ПДн	не установлено	подп. «а» п. 9
	2 типа	специальные категории субъектов ПДн, не являющихся сотрудниками оператора ПДн	более 100000	подп. «б» п. 9

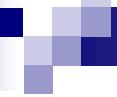
Уровень защищенности	Тип угрозы	Категория обрабатываемых ПДн	Количество обрабатываемых данных	Требования по защите (ПП № 1119)
2	1 типа	общедоступные	не установлено	подп. «а» п. 10
	2 типа	специальные категории ПДн сотрудников организации	не установлено	подп. «б» п. 10
		специальные категории субъектов ПДн, не являющихся сотрудниками оператора ПДн	менее чем 100000	подп. «б» п. 10
		биометрические	не установлено	подп. «в» п. 10
		общедоступные ПДн, не являющихся сотрудниками оператора ПДн	более 100000	подп. «г» п. 10
		иные категории ПДн, не являющихся сотрудниками оператора ПДн	более 100000	подп. «д» п. 10
3	3 типа	специальные категории субъектов ПДн, не являющихся сотрудниками оператора ПДн	более 100000	подп. «е» п. 10

Уровень защищенности	Тип угрозы	Категория обрабатываемых ПДн	Количество обрабатываемых данных	Требования по защите (ПП № 1119)
3	2 типа	общедоступные ПДн сотрудников оператора	не установлено	подп. «а» п. 11
		общедоступные ПДн, не являющихся сотрудниками оператора ПДн	менее 100000	подп. «а» п. 11
		иные категории ПДн сотрудников оператора	не установлено	подп. «б» п. 11
		иные категории ПДн, не являющихся сотрудниками оператора ПДн	менее 100000	подп. «б» п. 11
	3 типа	специальные категории ПДн сотрудников организации	не установлено	подп. «в» п. 11
		специальные категории субъектов ПДн, не являющихся сотрудниками оператора ПДн	менее чем 100000	подп. «в» п. 11
		биометрические	не установлено	подп. «г» п. 11
38		иные категории ПДн, не являющихся сотрудниками оператора ПДн	более 100000	подп. «д» п. 11

Уровень защищенностии	Тип угрозы	Категория обрабатываемых ПДн	Количество обрабатываемых данных	Требования по защите (Постановление № 1119)
4	3 типа	общедоступные	не установлено	подп. «а» п. 12
		иные категории персональных данных сотрудников оператора	не установлено	подп. «б» п. 12
		иные категории ПДн, не являющихся сотрудниками оператора ПДн	менее 100000	подп. «б» п. 12

Требования по защите ПДн в зависимости от уровня защищенности

Требование по защите ПДн	Уровни защищенности			
	1	2	3	4
Организация режима обеспечения безопасности помещений, в которых размещена ИС, препятствующая возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
Обеспечение сохранности носителей персональных данных	+	+	+	+
Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	+	+	+	+
Назначение должностного лица (работников), ответственного за обеспечение безопасности ПДн в ИС	+	+	+	
Ограничение доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в данном журнале, необходимы для выполнения служебных (трудовых) обязанностей	+	+		
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника по доступа к ПДн, содержащимся в ИС	+			
Создание структурного подразделения, ответственного за обеспечение безопасности ПДн в ИС, либо возложение на одно из структурных подразделений по обеспечению такой безопасности.	+			



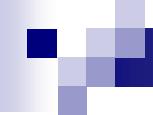
Класс специальной ИС

определяется на основе модели угроз безопасности ПД в соответствии с методическими документами, разрабатываемыми в соответствии с постановлением Правительства РФ от 17 ноября 2007 года N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах ПД"

Основные мероприятия по обеспечению безопасности специальных ИС включают:

- определение угроз безопасности ПД и формирование модели угроз;
- разработка на основе модели угроз системы защиты ПД;
- проверка готовности системы защиты информации (СЗИ) к использованию;
- обучение персонала правилам работы с СЗИ;
- учет применяемых СЗИ и носителей ПД;





- учет лиц, допущенных к работе с ПД;
- контроль за соблюдением условий использования СЗИ;
- реагирование на нарушение режима защиты ПД;
- описание системы защиты персональных данных.

Все перечисленное, за исключением первого пункта, необходимо выполнить и при внедрении типовой ИС.

Контрольные вопросы

- 1. Нормативно-правовое регулирование ПД в РФ.**
- 2. Проблемы защиты ПД.**
- 3. Способы обработки ПД.**
- 4. Порядок проведения классификации информационных систем ПД.**
- 5. Категории ПД.**
- 6. Значения параметра объема обрабатываемых ПД.**
- 7. Как определить класс типовой информационной системы в которой обрабатываются ПД?**
- 8. Назовите мероприятия, проводимые по обеспечению безопасности ИС.**

Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 8.2

- 1. Нормативно-правовое регулирование ПД в РФ.**
- 2. Проблемы защиты ПД.**
- 3. Способы обработки ПД.**
- 4. Порядок проведения классификации информационных систем ПД.**
- 5. Категории ПД.**
- 6. Значения параметра объема обрабатываемых ПД.**
- 7. Как определить класс типовой информационной системы в которой обрабатываются ПД?**
- 8. Назовите мероприятия, проводимые по обеспечению безопасности ИС.**

9. Нормативные документы в области защиты от киберпреступлений

9.1. Международные стандарты и соглашения в области безопасности информационных технологий

Важным элементом решения проблемы безопасности ИТ является **выработка системы требований**, критериев и показателей для оценки уровня безопасности ИТ в виде международного стандарта.

История создания данного стандарта.

В начале 80-х годов в США были разработаны "**Критерии оценки доверенных компьютерных систем**" (TCSEC).

В Европе в 1991г. были разработаны "**Критерии оценки безопасности информационных технологий**" (ITSEC) совместно Францией, Германией, Нидерландами и Великобританией.

В Канаде в начале 1993 г. были созданы "Канадские критерии оценки доверенных компьютерных продуктов" (CTCPEC).

В США в это же время был издан проект стандарта "Федеральные критерии безопасности информационных технологий" (FC), использовавший другой подход к объединению североамериканской и европейской концепций критериев оценки.

В 1990 г. Международная организация по стандартизации (ISO) начала разработку **международного стандарта критериев оценки для общего использования**. Версия 1.0 ОК была завершена ССЕВ в январе 1996 г. и одобрена ISO в апреле 1996 г. Бета-версия 2.0 ОК появилась в октябре 1997 г.

БАЗОВЫЕ ДОКУМЕНТЫ

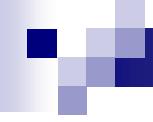


Рис. 1. Предыстория «Общих критериев»

В результате появился **Международный стандарт ISO/IEC 15408-99 "Критерии оценки безопасности информационных технологий" или так называемые "Общие критерии".**

В России аналогичный стандарт подготовлен в 2001г. Это ГОСТ Р ИСО/МЭК 15408-1-2001 **«Критерии оценки безопасности информационных технологий».**

Стандарт содержит **общие критерии (ОК)** оценки безопасности информационных технологий. Предназначен в качестве руководства при разработке и при приобретении **коммерческих** продуктов или систем с функциями безопасности ИТ.



ОК применимы к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. Критерии для оценки специфических качеств криптографических алгоритмов не входят в ОК

ОК безопасности продуктов и систем ИТ предназначены в основном для потребителей, разработчиков и оценщиков.

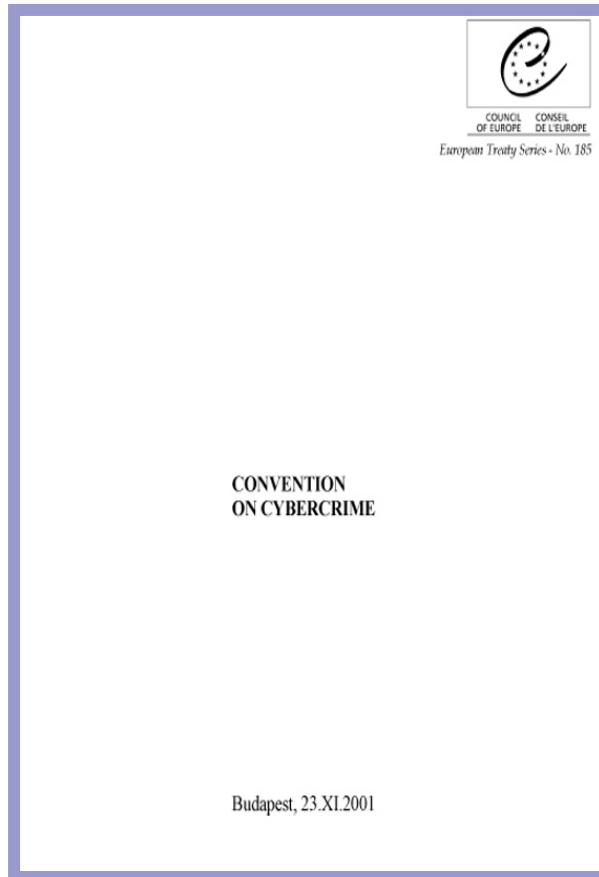
ОК предоставляют потребителям, независимую от реализации структуру, называемую **профилем защиты** (ПЗ), для выражения их специфических требований к мерам безопасности ИТ в объекте оценки.

В настоящее время действуют также и другие международные и российские стандарты

- ISO/IEC 17799 «Безопасность информационных систем»
- ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности»
- ГОСТ Р ИСО/МЭК 19794-2-2005» «Автоматическая идентификация. Идентификация биометрическая»
- ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»

- ГОСТ Р 51275-99 «Задача информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
- ГОСТ Р 51624-2000 «Автоматизированные системы в защищенном исполнении. Общие положения»
- ГОСТ Р 52447-2005 «Задача информации. Техника защиты информации»
- СТО БР МББС-1.0-2006 «Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»

В Будапеште в 23 ноября 2001 г. подписана **Конвенция по борьбе с киберпреступностью**. (26 европейских стран, а также Канады, США, ЮАР и Японии)



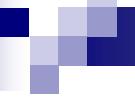
Конвенция разрабатывалась специальным комитетом Совета Европы при участии юристов США и других стран в течение 10 четырех лет

В конвенции представлена классификация киберпреступлений.

- ▶ Противозаконный доступ
- ▶ Неправомерный перехват
- ▶ Воздействие на данные
- ▶ Воздействие на функционирование системы
- ▶ Противозаконное использование устройств
- ▶ Подлог с использованием компьютерных технологий
- ▶ Мошенничество с использованием компьютерных технологий
- ▶ Правонарушения, связанные с детской порнографией
- ▶ Правонарушения, связанные с нарушением авторского права и смежных прав
- ▶ Покушение, соучастие или подстрекательство к совершению преступления

Россия не подписала Конвенцию Совета Европы из-за пункта "b" статьи 32:

"Страна может без согласия другой Страны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой страны компьютерным данным или получить их, если эта страна имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой стране через такую компьютерную систему "



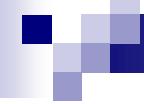
В Распоряжении Президента РФ сказано, что данные положения статьи

"могут причинить ущерб суверенитету и безопасности государств-участников конвенции и правам их граждан".

К настоящему времени Конвенцию подписали 47 стран, но ратифицировали только 24 страны.

Киберпреступления стали выгодным способом незаконного обогащения:

- ▶ **киберпреступники снимают деньги с банковских счетов граждан, обманывают банки с кредитными картами и занимаются промышленным шпионажем** путем создания преступных групп. (Одни люди специализируются на написании вредоносного кода, другие на рассылке спама, третьи на сдаче в аренду бот-сетей, четвертые на краже номеров кредитных карт, пятые на изготовлении поддельных пластиковых карт и т.д.);
- ▶ **при этом риски быть пойманным крайне малы.** Есть страны, например, Панама, в которых киберпреступники неуязвимы из-за недостатков в законодательстве.



Борьбой с компьютерными преступлениями в РФ занимается Управление «К» МВД

Управление наблюдает за Рунет, закрывая незаконно действующие сайты.

Управлением «К» ликвидируются до сотни сайтов в год со следующей статистикой:

28% – за распространение экстремистской информации, направленной на разжигание разного рода вражды;

27% – за нанесение вреда личности путем публикаций сведений личного или клеветнического характера;

24% – за распространение контрафакта.

Наибольшую группу (**41 %**) составляют сайты с детской порнографией.

9.2. Особенности и классификация компьютерных преступлений

Проблема:

при расследовании многих преступлений
в компьютерных системах **заключается**
в установлении самого факта
совершения преступления.

Особенность:

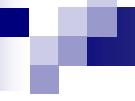
чтобы утверждать, что было совершено
преступление с использованием
компьютера, необходимо доказать
следующие факты:



- факт, что компьютерная информация, к которой произведен **несанкционированный доступ**, охраняется законами РФ;
- факт, что злоумышленником были осуществлены определенные **неправомерные действия**;
- факт, что этими несанкционированными действиями **нарушены права собственника информации**;
- факт несанкционированного **доступа к средствам компьютерной техники** либо попытка доступа;
- факт **использования информации в преступных целях**.
Например, с целью совершения преступления. Тогда **доказыванию подлежит**:
- факт, совершения несанкционированных манипуляций с программным обеспечением (ПО), что **лицо совершило их с преступной целью**.

Комплекс следственных действий включает:

- 1. Проведение обыска** в служебном помещении, на рабочем месте подозреваемого и изъятие физических носителей информации и других документов.
- 2. Исследование:** журнала рабочего времени ЭВМ, средств защиты и контроля регистрирующих систем пользователей, всего ПО ЭВМ, "прошитых" микросхем ПЗУ, микропроцессоров и т.п.
- 3. Анализ указаний** по обработке ежедневной бухгалтерской информации.

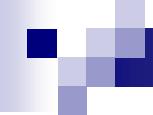
- 
- 4. Допрос инженеров** - программистов и специалистов электронщиков, занимающихся эксплуатацией и ремонтов вычислительной техники.
 - 5. Проведение комплексной судебно-бухгалтерской и программно-технической экспертизы** с привлечением соответствующих специалистов правоохранительных органов.

**Судебно-бухгалтерская экспертиза устанавливает
нарушения в документообороте, их причины и
ответственные лица за эти нарушения.**

**Результаты программно-технической экспертизы играют
роль доказательств в процессе суда.**

С помощью таких экспертиз решаются задачи:

- 1. Воспроизведение информации**, содержащейся на физических носителях.
- 2. Восстановление информации**, ранее содержавшейся на физических носителях и в последствии стертой или измененной по различным причинам.
- 3. Установление времени** ввода, изменение, уничтожение либо копирование той или иной информации.
- 4. Расшифровка закодированной информации**, подбор паролей и раскрытие систем защиты.



- 5. Установление авторства, места, средства, подготовки и способа изготовления документов (файлов, программ).**
- 6. Выяснения возможных каналов утечки информации из компьютерной сети и помещений.**
- 7. Выяснение технического состояния, исправности программно-аппаратных комплексов, возможности их адаптации под конкретного пользователя.**
- 8. Установления уровня профессиональной подготовки отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.**

Классификация способов совершения КП

По кодификатору **Интерпола** с 1991 г. все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы **Q**.

QA - Несанкционированный доступ и перехват

QD - Изменение компьютерных данных

QF - Компьютерное мошенничество

QR - Незаконное копирование

QS - Компьютерный саботаж

QZ - Прочие компьютерные преступления

В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время используется в более чем 100 странах.

- **QA - Несанкционированный доступ и перехват**
- **QAH** - компьютерный абордаж
- **QAI** - перехват
- **QAT** - кража времени
- **QAZ** - прочие виды несанкционированного доступа и перехвата
- **QD - Изменение компьютерных данных**
- **QUL** - логическая бомба
- **QDT** - троянский конь
- **QDV** - компьютерный вирус
- **QDW** - компьютерный червь
- **QDZ** - прочие виды изменения данных
- **QF - Компьютерное мошенничество**
- **QFC** - мошенничество с банкоматами
- **QFF** - компьютерная подделка
- **QFG** - мошенничество с игровыми автоматами
- **QFM** - манипуляции с программами ввода-вывода
- **QFP** - мошенничества с платежными средствами
- **QFT** - телефонное мошенничество
- **QFZ** - прочие компьютерные мошенничества
- **QR - Незаконное копирование**
- **QRG** - компьютерные игры
- **QRS** - прочее программное обеспечение
- **QRT** - топография полупроводниковых изделий
- **QRZ** - прочее незаконное копирование
- **QS - Компьютерный саботаж**
- **QSH** - с аппаратным обеспечением
- **QSS** - с программным обеспечением
- **QSZ** - прочие виды саботажа
- **QZ - Прочие компьютерные преступления**
- **QZB** - с использованием компьютерных досок объявлений
- **QZE** - хищение информации, составляющей коммерческую тайну
- **QZS** - передача информации конфиденциального характера
- **QZZ** - прочие компьютерные преступления

Для характеристики преступления могут использоваться до пяти кодов. Например, несанкционированный доступ и перехват информации (QA) включает в себя следующие виды КП:

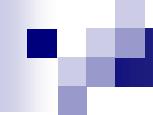
QAH - "Компьютерный абордаж" (хакинг - hacking): неправомерный доступ в компьютер или сеть.

QAI - перехват (interception): перехват при помощи технических средств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, системы спутниковой связи, а также специальные системы правительственный связи. К данному виду КП также относится электромагнитный перехват (electromagnetic pickup).

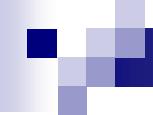
QAT - кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая терминология:

- ▶ **"Жучок"** (bugging) - установка микрофона в компьютере;
- ▶ **"Откачивание данных"** (data leakage) - возможность сбора информации, для получения данны, о технологии ее прохождения в системе;
- ▶ **"Уборка мусора"** (scavenging) - поиск данных, оставленных пользователем после работы на компьютере (в мусорных корзинах, в памяти машины);
- ▶ метод следования **"За дураком"** (piggybacking), характеризующий несанкционированное проникновение как в закрытые зоны. Его суть: дождавшись законного пользователя, можно пройти в дверь помещения вместе с НИМ;



- ▶ метод "**За хвост**" (between the lines entry). Подключаются к линии связи законного пользователя, когда последний заканчивает активный режим, и осуществляют доступ к системе;
- ▶ метод "**Несспешного выбора**" (browsing). Путем несанкционированный доступ к базам данных путем нахождения слабых мест в защите систем;
- ▶ метод "**Поиск бреши**" (trapdoor entry). Используются ошибки в логике построения программы;



- ▶ метод "**Люк**" (trapdoor). В найденной "брееши" (в предыдущем методе) программа "разрывается" и туда вставляется определенное число команд;
- ▶ метод "**Маскарад**" (masquerading). В этом случае злоумышленник проникает в компьютерную систему, выдавая себя за законного пользователя;
- ▶ метод "**Мистификация**" (spoofing). Используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, поддерживает заблуждение ошибочно подключившегося пользователя и получает полезную информацию.

Анализ компьютерных преступлений

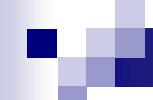
Диапазон компьютерных преступлений в настоящее время расширился и включает кроме традиционного мошенничества также **киберслежку, мошенничество с инвестициями, сексуальные домогательства, кражу информации, внутригосударственный и международный терроризм, нарушение авторских прав, фальсификацию систем, насильственные преступления, жестокое обращение с пожилыми.**

С целью совершенствования методов расследования, правоохранительные органы проводят **анализ КП**.
Создаются системы адаптации «традиционных» методов расследования преступлений с использованием компьютерных средств.

Для предупреждения преступлений используются региональные и международные средства анализа. Эти системы могут объединять преступления по местоположению, времени и методу действий, что может помочь **прогнозировать потенциальные будущие угрозы.**

Например, в университете Карнеги-Меллона создана группа «скорой компьютерной помощи» Computer Emergency Response Team (CERT), которая ставит своей целью анализ и разработку **мер противодействия** компьютерным преступлениям.

Проделанная этой группой работа показывает, что **понимание целей, которые ставит перед собой злоумышленник, позволяет определять его будущие поступки.**



Для выявления нарушений системной защиты **используются методы активной добычи данных.**

При этом проводят **анализ поступков, которые приводят к нарушениям**, и сравнивают их с поведением при нормальной работе.

Собирается **информация о часто встречающейся последовательности действий.**

Эти **сведения используются для создания автоматического классификатора**, который способен различать агрессивное и нормальное поведение.

9.2. Требования к безопасности компьютерных сетей в РФ

Эти требования разработаны ГТК РФ и обязательны для государственных предприятий или для коммерческих предприятий допущенных к сведениям составляющих ГТ. В остальных случаях они носят рекомендательный характер.

К таким документам относится, например, РД ГТК «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» от 30.03.92.

Установленные классы регламентируют использование в АС следующих подсистем:

- управления доступом;
- криптографической;
- регистрации и учета;
- обеспечения целостности.

Требования к безопасности АС устанавливаются в соответствии с классом защищенности.

Установлено 9 классов защищенности в трех группах:
3Б, 3А, 2Б, 2А, 1Д, 1Г, 1В, 1Б, 1А.

3-я группа - в АС работает 1 пользователь, допущенный к информации одного уровня конфиденциальности;

2-я группа – в АС пользователи имеют одинаковые права к информации различного уровня конфиденциальности;

1-я группа – многопользовательские системы с доступом к информации разного уровня.



Показатели защищенности средств вычислительной техники от НСД даны в РД ГТК «Средства ВТ. Защита от НСД. Показатели защищенности от НСД к информации» от 30.03.92.

В данном РД определяется 7 классов защищенности СВТ от НСД к информации.

Самый высокий – 1, самый низкий – 7 класс.

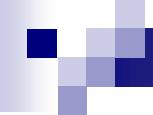
Классы подразделяются на 4 группы:

1 гр. включает – 7 кл.,

2 гр. включает – 6 и 5 кл.,

3 гр. включает – 4, 3 и 2 кл.,

4 гр. включает – 1 кл.



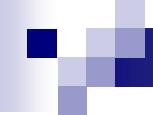
Для присвоения класса защищенности АС должна иметь:

- ▶ руководство администратора по системе;
- ▶ руководство пользователя;
- ▶ тестовую и конструкторскую документацию.

Кроме этого действуют следующие РД ГТК:

- ▶ "Защита от НСД к информации. Термины и определения". Решение Председателя ГТК от 30.03.92г.
- ▶ "Концепция защиты СВТ и АС от НСД к информации". Решение Председателя ГТК от 30.03.92г.
- ▶ "Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники". Решение Председателя ГТК от 30.03.92г.

- ▶ "Средства вычислительной техники. **Межсетевые экраны**. Защита от НСД к информации. Показатели защищенности от несанкционированного доступа к информации". Решение Председателя ГТК от 25.07.97г.
- ▶ "Защита информации. **Специальные защитные знаки**. Классификация и общие требования". Решение Председателя ГТК от 25.07.97г.
- ▶ "Защита от НСД к информации. **Программное обеспечение средств защиты информации**. Классификация по уровню контроля отсутствия недекларированных возможностей" (введен в действие приказом Председателя Гостехкомиссии России №114 от 4.06.99 г.)
- ▶ "Специальные требования и рекомендации по технической защите конфиденциальной информации". 2001г.



Для корпоративных сетей с большим количеством пользователей составляется документ, регламентирующий работу в сети – **«Политика безопасности»**.

Политика безопасности отражает собственную концепцию защиты информации организации и разрабатывается на основе:

- ▶ РД ГТК,
- ▶ требований стандартов безопасности (ISO 17799),
и
- ▶ стандартов качества (ISO 9000).

В "Оранжевой книге" политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

На практике политика безопасности трактуется несколько шире - как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса и содержит следующие сведения:

- ▶ основные положения информационной безопасности;
- ▶ область применения;
- ▶ цели и задачи обеспечения ИБ;
- ▶ распределение ролей и ответственности;
- ▶ общие обязанности.

«Политика безопасности» обеспечивает выполнение следующих правил безопасности информации:

- Идентификация
- Разделение полномочий
- Регистрация и учет работы
- Шифрование
- Применение цифровой подписи
- Обеспечение антивирусной защитой
- Контроль целостности информации

При этом обеспечивается выполнение трех основных функций системы:

доступность, целостность, конфиденциальность.

Политику безопасности имеет два-три уровня

Верхний уровень определяет политику организации в целом.

На указанном уровне формулируются главные цели информационной безопасности (определяемые сферой деятельности предприятия): обеспечение конфиденциальности, целостности и доступности.

Средний уровень политики безопасности выделяют в случае структурной сложности организации или наличии специфичные подсистемы организации.

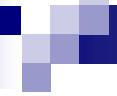
Например, наличие подразделений **обрабатывающих секретную информацию**.

За разработку и реализацию политики безопасности верхнего и среднего уровней **отвечают руководитель службы безопасности, администраторы безопасности АС и ВС.**

Нижний уровень относится к конкретным службам или подразделениям организации.

На нижнем уровне описываются механизмы защиты информации и программно-технические средства для их реализации.

За политику безопасности нижнего уровня **отвечают системные администраторы (администраторы безопасности).**



9.3. Требования к созданию системы обеспечения информационной безопасности предприятия

Создание системы информационной безопасности (СИБ) на предприятии включают следующие этапы:

- 1- разработка политики безопасности;**
- 2- проведение анализа рисков;**
- 3- планирование обеспечения ИБ, планирование действий в чрезвычайных ситуациях;**
- 4- подбор механизмов и средств обеспечения ИБ.**

Первые два этапа составляют так называемый административный уровень системы.

Третий и четвертый этапы заключаются в **разработке процедур безопасности** (практических мер по реализации СИБ).

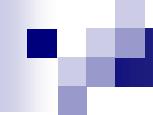
Цели и задачи СБИ вытекают из функционального назначения предприятия.

Например:

для режимных организаций на первое место ставится **конфиденциальность**;

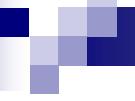
для сервисных информационных служб - **доступность** подсистем;

для информационных хранилищ - **целостность** данных и т д.



Типовыми целями СИБ могут быть например:

- ▶ **обеспечение уровня безопасности, соответствующего нормативным документам предприятия;**
- ▶ **достижение экономической целесообразности в выборе защитных мер;**
- ▶ **обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС.**



На 1 этапе создания СИБ конкретизируются стратегические принципы безопасности (вытекающие из целей и задач),

например:

- ▶ **"защититься и продолжить"**, когда организация оказывает максимальное противодействие нарушению;
- ▶ **"выследить и осудить"**, когда злоумышленнику позволяют продолжить действия с целью его выявления и наказания.

Обстоятельства, позволяющие выбрать стратегию

Защититься и продолжить	Выследить и осудить
<ul style="list-style-type: none">• АС недостаточно защищены.• Продолжительность вторжения сопряжена с финансовым риском.• Неизвестен круг пользователей.• Пользователей могут привлечь к ответственности за нанесенный ущерб и др.	<ul style="list-style-type: none">• АС хорошо защищена, используются надежные средства резервирования.• Имеют место повторяющиеся и частые атаки.• Действия злоумышленника можно контролировать.• Организация обладает положительным опытом работы с правоохранительными и правозащитными органами и др.

Для каждой категории пользователей указывается **правило пользования ресурсом** принято в организации (выбирается из двух вариантов):

- ◆ что явно не запрещено, то разрешено;
- ◆ что явно не разрешено, то запрещено.

Утверждается **схема доступа** к сервисам:

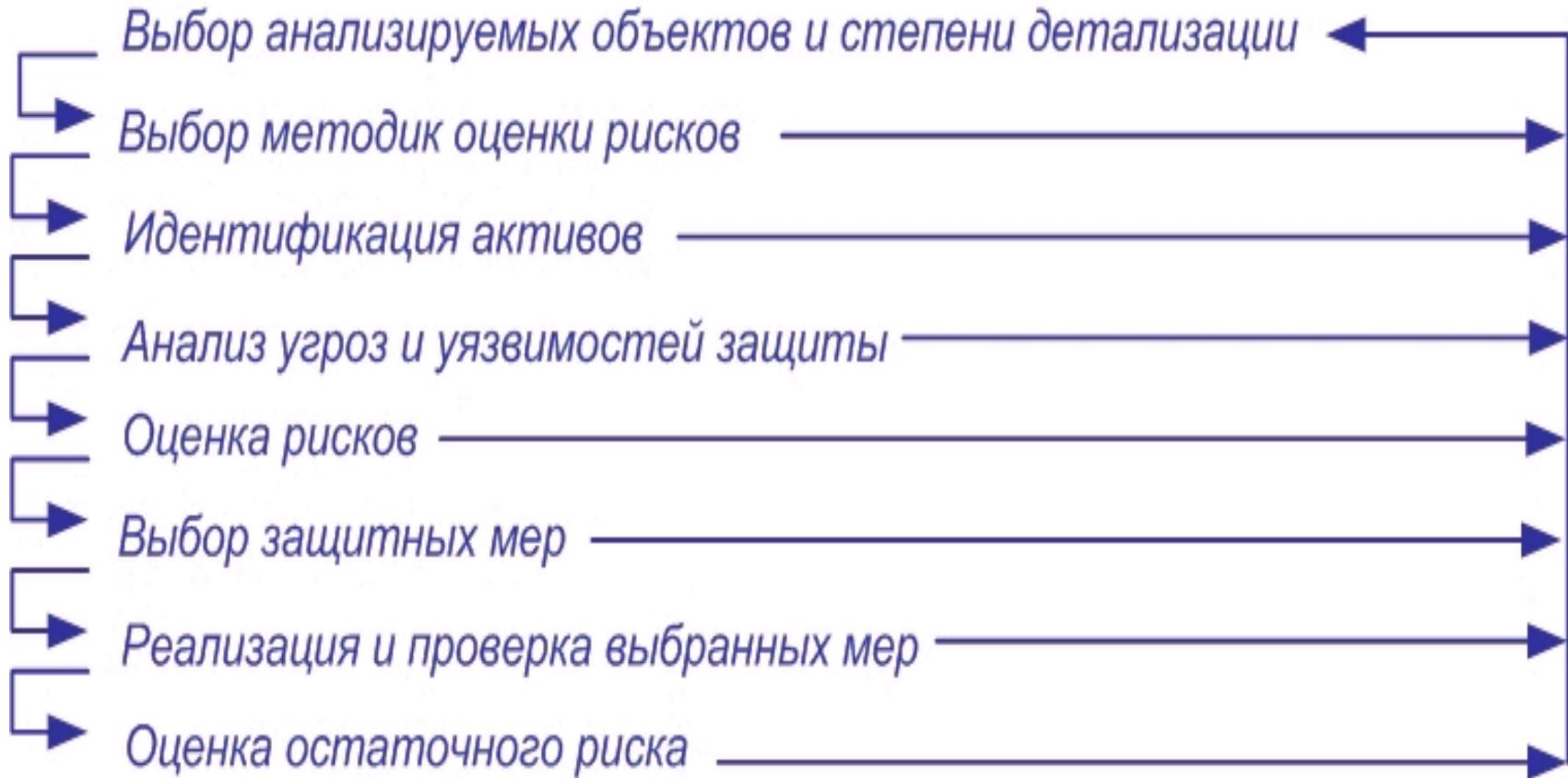
- ◆ централизованная;
- ◆ децентрализованная;
- ◆ иная.

Проведение анализа риска

Под рисками, понимаются стоимостьные (вероятностные) выражения событий, ведущих к потерям. Если риск не приемлем, то необходимо предпринять защитные меры, не превышающие по стоимости возможный ущерб.

Анализ риска необходим для выявления уязвимости АС, определения затрат на СИБ, выбора мер и средств защиты, а также повышения компетентности персонала АС.

Схема анализа риска



Идентификация активов

В основе анализа риска лежит определение того, что надо защищать, от кого и как. Для этого выявляются **активы АС**, нуждающиеся в защите

Категории активов	Компоненты АС
Аппаратное обеспечение	Компьютеры, периферийные устройства, коммуникационные линии, сетевое оборудование и их составные части
Программное обеспечение	Исходные, объектные и загрузочные модули операционных систем, вспомогательных системных и коммуникационных программ, инструментальных средств разработки, прикладных программных пакетов
Информационное обеспечение	Вводимые и обрабатываемые, хранимые, передаваемые и резервные (сохраненные копии) данные и метаданные
Персонал	Обслуживающий персонал и пользователи
Документация	Конструкторская, техническая, пользовательская и иная документация
Расходные материалы	Бумага, магнитные носители, картриджи и т.д.

При анализе угроз необходимо выявить их источники и условия реализации.

Внешние источники угроз	Внутренние источники угроз
<p>1.Атмосферные явления, стихийные бедствия, катастрофы, аварии,</p> <p>2.Деятельность конкурирующих экономических структур,</p> <p>3.Деятельность преступных группировок и лиц и др.</p>	<p>1.Нарушение персоналом режимов безопасности</p> <p>2.Отказы и сбои аппаратных средств и носителей информации,</p> <p>3.Ошибки программного обеспечения,</p> <p>4.Злоумышленная деятельность персонала.</p>

Оценка рисков

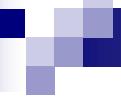
Количественную **оценку риска** можно получить путем
экспертного опроса, статистически или по
математической зависимости.

Ожидаемые потери рассчитываются по следующей
формуле:

$$E = V \cdot p, \text{ где}$$

p – вероятность возникновения угрозы;

V - оценка ущерба при реализации угрозы.



**Если задан коэффициент защищенности СИБ (Кз)
(например, Кз может быть 85%, 90% и т.п.)**

Тогда можно оценить величину ущерба при реализации угрозы используемым активам:

$$V = S \cdot (1 - Kz),$$

где **S** – стоимость актива.

Способы оценки вероятностей возможных потерь

- 1. Методы экспертных оценок** (применяются при оценке трудно предсказуемых угроз).
- 2. Методика определения приемлемости уровня риска по трехбалльной шкале.**
- 3. Методика определения приемлемости уровня риска с учетом видимости угроз и их последствий.**
- 4. Статистическая оценка событий и использование статистических моделей.**
- 5. Использование аналитических моделей потенциального ущерба.**
- 6. Методики оценки, на основе многофакторных испытаний.**



Основная задача методов анализа риска - оценить уровень возможных потерь и затрат на защиту.

Выбор и проверка защитных мер

Для уменьшения размера ущерба производится выбор мер защиты: организационных, физических, программно-технических и др.

Задача анализа и синтеза мер, методов и средств защиты решается **по критерию эффективность/стоимость**.

После выбора способов защиты АС производится проверка их эффективности. Если остаточные риски стали опять-таки неприемлемы, повторяют этапы анализа риска.



При создании системы безопасности используется необходимо:

- определить объекты защиты, уничтожение или модификация которых, может привести к уменьшению прибыли;
- определить угрозы безопасности защищаемых объектов;
- оценить вероятность и частоту данных угроз;
- выбрать адекватные средства и методы защиты.

Основные элементы процесса защиты - объекты защиты, виды злоумышленников (ЗЛ) и их возможности, определенные рубежами защиты представлены в таблице.

Объекты защиты	ЗЛ за предела ми КЗ	Положение ЗЛ			
		ЗЛ в пределах контролируемой зоны (КЗ)			
		ЗЛ в пределах КЗ	ЗЛ в выделенном помещении	ЗЛ - сотрудник объекта	ЗЛ – сотрудник СБ
Человек	Гр. 4, 5, 7, 8	Гр. 5	Гр. 5	Гр. 5	Гр. 5
Информация	Гр. 3, 8, 9	Гр. 3, 6, 9	Гр. 3, 6, 9	Гр. 3, 6, 9	Гр. 3, 6, 9
Материаль-ные ценности	Гр. 1, 8	Гр. 1, 2	Гр. 1, 2	Гр. 1, 2	Гр. 1, 2

Захита от каждого вида злоумышленников реализуется путем создания службы безопасности.

В состав СБ предприятия входят следующие подразделения (в скобках указаны номера групп, указанных в таблице):

- группа охраны (Гр. 1);
- служба пожарной охраны (Гр. 2);
- группа противодействия технической разведки (Гр. 3);
- детективная группа (Гр. 4);
- группа режима (Гр. 5);
- кризисная группа (Гр. 6);
- служба личной охраны (Гр. 7);
- аналитическая группа (Гр. 8);
- группа защиты от НСД (Гр. 9);
- группа по работе с кадрами (Гр. 10);
- группа защиты информации (Гр. 11).

Оптимальная СИБ создается на основе решения технико-экономических задач защиты информации.

1. На основе опыта создания СИБ, составляются варианты наборов средств, решающих поставленную задачу.
2. Выбираются наиболее подходящие варианты, решающие задачи защиты информации на всех рубежах.
3. На основе технико-экономических оценок средств защиты определяются размеры ресурсов, необходимых для практического использования различных средств.

Контрольные вопросы

1. Международные стандарты и соглашения в области безопасности ИТ.
2. Назовите особенности расследования КП.
3. Какие задачи решаются судебно-бухгалтерской и техническими экспертизами при проведении расследований КП?
4. Методы и приемы предупреждения КП. Анализ компьютерных преступлений.
5. Требования к безопасности компьютерных сетей в РФ.
6. На основе каких документов разрабатывается Политика безопасности? Уровни Политики безопасности.
7. Исходя из чего выбирают стратегические принципы безопасности?
8. Зачем проводится анализ риска? Методы оценки рисков.
9. Категории защищаемых активов АС, классификация угроз.

Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 9

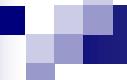
1. Международные стандарты и соглашения в области безопасности ИТ.
2. Назовите особенности расследования КП.
3. Какие задачи решаются судебно-бухгалтерской и техническими экспертизами при проведении расследований КП?
4. Методы и приемы предупреждения КП. Анализ компьютерных преступлений.
5. Требования к безопасности компьютерных сетей в РФ.
6. На основе каких документов разрабатывается Политика безопасности? Уровни Политики безопасности.
7. Исходя из чего выбирают стратегические принципы безопасности?
8. Зачем проводится анализ риска? Методы оценки рисков.
9. Категории защищаемых активов АС, классификация угроз.

Тема 10

Зашита интеллектуальной собственности

10.1. Объекты интеллектуальной собственности

Интеллектуальная собственность (ГК часть 1, ст.138) -
исключительное право гражданина или юридического
лица на результаты интеллектуальной деятельности и
приравненные к ним **средства индивидуализации**
юридического лица,
индивидуализации продукции,
выполненных работ или услуг
(фирменное наименование, товарный знак и т.п.).

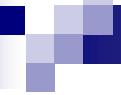


Уточнения даны в **4-й части ГК РФ**, принятой 18.12.2006г.
№ 230.

**Результатами интеллектуальной деятельности и
приравненными к ним средствами индивидуализации
юридических лиц, товаров, работ, услуг и предприятий,
которым предоставляется правовая охрана
(интеллектуальной собственностью), являются:**

- 1) произведения науки, литературы и искусства;**
- 2) программы для электронных вычислительных
машин (программы для ЭВМ);**
- 3) базы данных;**
- 4) исполнения;**
- 5) фонограммы;**

- 6) сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);**
- 7) изобретения;**
- 8) полезные модели;**
- 9) промышленные образцы;**
- 10) селекционные достижения;**
- 11) топологии интегральных микросхем;**
- 12) секреты производства (ноу-хау);**
- 13) фирменные наименования;**
- 14) товарные знаки и знаки обслуживания;**
- 15) наименования мест происхождения товаров;**
- 16) коммерческие обозначения.**



На результаты интеллектуальной деятельности признаются интеллектуальные права, которые включают:

исключительное право, являющееся имущественным правом и личные неимущественные права
(называемые автором).



Существует три общепризнанные в мире правовые формы защиты объектов интеллектуальной собственности (**ОИС**):

авторское право,

патентное право, и

секреты производства.

Авторское право - форма правовой защиты в отношении литературных, художественных и научных произведений.

Патентное право - форма правовой защиты в отношении изобретений во всех областях человеческой деятельности.

Секреты производства (ноу-хай) – форма правовой защиты любых полезных сведения (производственных, технических, экономических, организационных и других).

Историческая справка

Первый закон об авторском праве был принят в Англии в 1710 году. Охрана личных прав давалась на 14 лет с продлением еще на 14 лет.

Первым патентным законом была Декларация Венецианской республики в 1474г. Изобретатель получал привилегию (патент) на 10 лет.

В России выдача привилегий началась с 1748г. Общий закон «О привилегиях...» появился в 1812г.

В РФ до недавнего времени действовали следующие законодательные акты, защищающие права граждан и юридических лиц на ОИС.

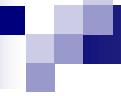
1. Закон РФ “Об авторском праве и смежных правах”, от 9.07.93г. №5351-1 (редакция от 20.07.04г. №72).
2. Закон РФ “Патентный закон РФ”, от 23.09.92г. № 3517-1.
3. Закон РФ “О правовой охране программ для ЭВМ и баз данных”, от 23.09.92г. №3523-1.
4. Закон РФ “О правовой охране топологий интегральных микросхем”, от 23.09.92г. №3526-1.
5. Закон РФ “О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров”, от 23.09.92г. № 3520-1.
6. Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”, от 22.03.91г. №948-1. (Ред. от 9 октября 2002 г №122-ФЗ).
7. Закон РФ "О защите конкуренции", от 26.07.2006г. N135-ФЗ.

После вступления в силу с 1 января 2008г 4-й части Гражданского кодекса РФ большинство указанных выше законов РФ, касающихся защиты ИС, потеряло силу.

Заключены следующие международные конвенции и соглашения, связанные с охраной интеллектуальной собственности:

- 1. Конвенция по охране промышленной собственности** от 20 марта 1883г. (редакция от 2 октября 1979г.), заключенная в Париже.

- 2. Конвенция по охране литературных и художественных произведений** от 9 сентября 1886г., заключенная в Берне (последняя редакция 1971г.).



- 3. Конвенция о международной регистрации фабричных и товарных знаков от 14 апреля 1891г. (редакция от 2 октября 1979г.), заключенная в Мадриде.**
- 4. Всемирная (Женевская) конвенция об авторском праве от 6 октября 1952г., заключенная в Женеве.**
- 5. Конвенция по охране интересов производителей фонограмм от незаконного воспроизведения фонограмм от 29 октября 1971г., заключенная в Женеве.**
- 6. Конвенция, учреждающая всемирную организацию интеллектуальной собственности от 14 июля 1967г. (редакция 2 октября 1979г.), заключенная в Стокгольме.**

- 7. Брюссельская конвенция о распространение несущих сигналов, передаваемых через спутники от 21.мая 1974г.**
- 8. Евразийская патентная конвенция 1994 г.**
- 9. Гаагское соглашение по международному депонированию промышленных образцов от 28 ноября 1960г. (редакция от 2 октября 1979г.).**
- 10. Международная конвенция об охране интересов исполнителей, производителей фонограмм и вещательных организаций, заключенной в Риме 26 октября 1961г. ("Римская конвенция").**
РФ не участвует в двух последних.

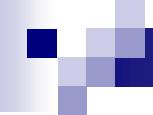
Были созданы организации и союзы по охране ИС:

-Международное бюро по ИС;

-Всемирная Организация Интеллектуальной Собственности (ВОИС);

-Международный союз по охране промышленной собственности (Парижский Союз), образованный Парижской конвенцией по охране промышленной собственности;

-Международный союз (Бернский Союз), образованный Бернской конвенцией по охране литературных и художественных произведений.



Автором результата интеллектуальной деятельности признается гражданин, творческим трудом которого создан такой результат.

Автору результата интеллектуальной деятельности принадлежит право авторства, право на имя и иные личные неимущественные права.

Авторство и имя автора охраняются бессрочно.

Исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора.

Это право может быть передано автором другому лицу по договору, а также может **перейти к другим лицам** по иным основаниям, установленным законом.

Права на результат интеллектуальной деятельности, созданный совместным творческим трудом двух и более граждан, **принадлежат соавторам совместно.**

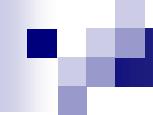


10.2. Правовые нормы защиты интеллектуальной собственности

ПРАВОВАЯ ОХРАНА АВТОРСКИХ И СМЕЖНЫХ ПРАВ

Закон регулирует отношения, возникающие при создании и использовании произведений науки, литературы и искусства (**авторское право**),

фонограмм исполнителей, постановок, передач организаций эфирно или кабельного вещания (**смежные права**).



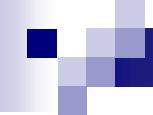
Интеллектуальные права на произведения науки, литературы и искусства являются авторскими правами.

Автору произведения принадлежат следующие права:

- **исключительное право** на произведение;
- **право авторства;**
- **право автора на имя;**
- **право на неприкосновенность произведения;**
- **право на обнародование произведения.**

Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой либо объективной форме:

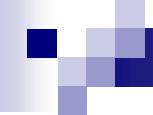
- письменной;**
- устной** (выступление, исполнение и т.д.);
- звуко- или видеозаписи;**
- изображения** (рисунок, чертеж, теле-, фотокадр и т.д.);
- объемно-пространственной** (скульптура, макет и т.д.);
- в других формах.**



К объектам авторских прав также относятся
программы для ЭВМ, которые охраняются как
литературные произведения.

Автор - физическое лицо, творческим трудом
которого создано произведение.

Авторское право не распространяется на идеи,
методы, процессы, системы, концепции, принципы,
открытия, факты.



Не являются объектами авторского права:

- официальные документы** (законы, судебные решения и т.п.);
- государственные символы и знаки** (флаги, гербы, ордена и т.п.);
- произведения народного творчества;**
- сообщения о событиях и фактах, имеющие информационный характер.**

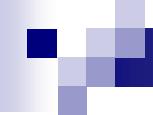
Авторское право на произведение возникает в силу факта его создания.

Для возникновения и осуществления авторского права не требуется регистрации произведения или соблюдения каких - либо формальностей.

В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя (в соответствии с правилами статьи 1262 Гражданского Кодекса).

Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать **знак охраны авторского права**, который помещается на каждом экземпляре произведения и состоит из трех элементов:

- буквы “С” в окружности ©;**
- имени (наименования) обладателя исключительных прав;**
- года первого опубликования произведения.**



**При опубликовании произведения
анонимно или под псевдонимом
представителем автора является
издатель, который имеет право защищать
права автора пока автор не раскроет свою
личность.**



При соавторстве (произведение создано двумя и более лицами) авторское право принадлежит соавторам совместно, независимо от характера и структуры произведения (неразрывное целое или имеет отдельные самостоятельные части).

Если произведение создано в порядке выполнения служебных обязанностей, **(служебное произведение)** то авторское право на него принадлежит автору служебного произведения, а исключительные права на его использования - работодателю.

Авторское **вознаграждение** при этом **определяется договором** между автором и работодателем.

Автору в отношении его произведений принадлежат личные неимущественные права (право признаваться автором, право обнародовать или разрешать обнародовать произведения, право на защиту произведения от искажения и др. посягательств) и **исключительные имущественные права** (право на использование - воспроизводить, показывать, исполнять, распространять и т.д.).

Авторское право действует в течении всей жизни автора и 70 лет после его смерти.

Историческая справка

В сфере авторского права до 70-х годов прошлого века в России срок действия исключительных прав составлял **15 лет** после смерти автора, с 1973 г. был увеличен до **25 лет**.

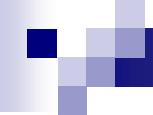
В 1991 г. в «Основах гражданского законодательства Союза ССР» срок действия авторских прав составил **50 лет**.

В 2004 г. были приняты поправки к Закону РФ “Об авторском праве и смежных правах” где действие авторского права установлено с учетом действующих международных норм в течении всей жизни автора и **70 лет** после его смерти.

Поправки, вступившие в силу с 1 сентября 2006 г., означают, что размещенные в сети, например, тексты книг или музыкальные файлы в формате mp3 охраняются авторским правом так же, как обычные книги или компакт-диски.

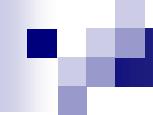
Они подпадают под действие ст. 146 Уголовного кодекса РФ ("Нарушение авторских и смежных прав"), предусматривающей наказание для пиратов в виде **лишения свободы на срок до шести лет.**

Владельцы тр3-сайтов теперь должны подписать лицензионные соглашения со всеми поставщиками музыки.



Истечение срока действия авторского права на произведения означает их переход в общественное достояние.

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно.



Знак охраны смежных прав – буква “Р” в окружности, имя обладателя прав и год первого опубликования фонограммы.

Исключительное право на исполнение
действует в течение всей жизни исполнителя, но **не менее пятидесяти лет**, считая с 1 января года, следующего за годом, в котором осуществлены исполнение, либо запись исполнения, либо сообщение исполнения в эфир или по кабелю.

По истечении срока действия исключительного права на исполнение это право переходит в общественное достояние.

Исключительное право на фонограмму действует в течение пятидесяти лет, считая с 1 января года, следующего за годом, в котором была осуществлена запись.

В соответствии с законом запрещается импортировать экземпляры фонограмм в целях распространения, передельывать, продавать и воспроизводить без разрешения их правообладателей.

Для включения механизма защиты смежных прав **необходимо заявление обладателя прав о нарушении его прав** (т.к. многие фирмы этого не делали, то до недавнего времени около 90% пиратской продукции на рынке считалось законной).

Обладатели исключительных или смежных прав вправе требовать от нарушителя: признания своих прав, возмещения убытков, взыскание полученного дохода, выплаты компенсации в размере от десяти тысяч рублей до пяти миллионов рублей, определяемом по усмотрению суда.

Статья 146 УК РФ. Нарушение авторских и смежных прав

1. Присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору или иному правообладателю , - **наказывается**

штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо арестом на срок от трех до шести месяцев.

Статья 146 УК РФ. Нарушение авторских и смежных прав

2. Незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере, - наказываются

штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо лишением свободы на срок до двух лет.

Статья 146 УК РФ. Нарушение авторских и смежных прав

3. Деяния, предусмотренные частью второй настоящей статьи, **если они совершены:**

- **группой лиц по предварительному сговору или организованной группой;**
- **в особо крупном размере;**
- **лицом с использованием своего служебного положения, - наказываются**

лишением свободы на срок до шести лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.

Объектами смежных прав являются:

- 1) исполнения артистов-исполнителей и дирижеров, постановки режиссеров - постановщиков спектаклей;**
- 2) фонограммы, то есть любые исключительно звуковые записи исполнений, за исключением звуковой записи, включенной в аудиовизуальное произведение;**
- 3) сообщения передач организаций эфирного или кабельного вещания;**
- 4) базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов;**
- 5) произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние, в части охраны прав публикаторов таких произведений.**

Для возникновения, осуществления и защиты смежных прав не требуется регистрация их объекта или соблюдение каких-либо иных формальностей.

Вознаграждение за свободное воспроизведение фонограмм и аудиовизуальных произведений в личных целях распределяется между правообладателями в следующей пропорции (статья 1245 ГК РФ). :

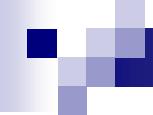
сорок процентов - авторам,

тридцать процентов - исполнителям,

тридцать процентов - изготовителям фонограмм или аудиовизуальных произведений.

Свободное воспроизведение произведения в личных целях допускается без согласия автора и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях, за исключением (статья 1273):

- 1) воспроизведения произведений архитектуры в форме зданий и аналогичных сооружений;**
- 2) воспроизведения баз данных или их существенных частей;**
- 3) воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 ГК (для исследовательских целей);**



- 4) **репродуцирования книг (полностью) и нотных текстов;**
- 5) **видеозаписи аудиовизуального произведения при его публичном исполнении в месте, открытом для свободного посещения, или в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи;**
- 6) **воспроизведения аудиовизуального произведения с помощью профессионального оборудования, не предназначенного для использования в домашних условиях.**

Использование фонограммы, опубликованной в коммерческих целях

Публичное исполнение фонограммы, опубликованной в коммерческих целях, а также ее сообщение в эфир или по кабелю **допускаются без разрешения обладателя** исключительного права на фонограмму и обладателя исключительного права на зафиксированное в этой фонограмме исполнение, **но с выплатой им вознаграждения.**

Вознаграждение, предусмотренное настоящей статьей, **распределяется** между правообладателями в следующей пропорции:

пятьдесят процентов - исполнителям,
пятьдесят процентов - изготовителям фонограмм.

Право публикатора на произведение науки, литературы или искусства

Публикатором признается гражданин, который **правомерно обнародовал произведения науки, литературы или искусства**, ранее не обнародованного и перешедшего в общественное достояние либо находящегося в общественном достоянии в силу того, что оно не охранялось авторским правом.

Исключительное право публикатора на произведение возникает в момент обнародования этого произведения и **действует в течение двадцати пяти лет**, считая с 1 января года, следующего за годом его обнародования.

Контрольные вопросы

- 1. Назовите правовые формы охраны интеллектуальной собственности.**
- 2. Что понимается под исключительными правами на объекты интеллектуальной собственности?**
- 3. Международные конвенции и соглашения, связанные с охраной интеллектуальной собственности.**
- 3. Правовая охрана авторских и смежных прав.**
- 4. Что представляет собой знак охраны авторского права.**
- 5. Сток действия авторского права.**
- 6. Знак охраны смежных прав.**
- 7. Ответственность за нарушение авторских и смежных прав.**

Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 10.1

- 1. Назовите правовые формы охраны интеллектуальной собственности.**
- 2. Что понимается под исключительными правами на объекты интеллектуальной собственности?**
- 3. Международные конвенции и соглашения, связанные с охраной интеллектуальной собственности.**
- 4. Правовая охрана авторских и смежных прав.**
- 5. Что представляет собой знак охраны авторского права.**
- 6. Сток действия авторского права.**
- 7. Знак охраны смежных прав.**
- 8. Ответственность за нарушение авторских и смежных прав.**

ПРАВОВАЯ ОХРАНА ПРОГРАММ ДЛЯ ЭВМ И БАЗ ДАННЫХ

Впервые программы для ЭВМ и базы данных стали объектами авторского права в 1991г., когда были приняты **Основы гражданского законодательства СССР и республик.**

Закон “О правовой охране программ для ЭВМ и баз данных” №3523 от 23.09.92г. регулировал до 2008г. отношения, связанные с созданием, правовой охраной и использованием программ ЭВМ и баз данных.

Программы для ЭВМ и базы данных были отнесены Законом к объектам авторского права.

Правообладатель в течение срока действия исключительного права на программу для ЭВМ или на базу данных **может по своему желанию зарегистрировать такую программу или такую базу данных** в федеральном органе исполнительной власти по интеллектуальной собственности.

Программы для ЭВМ и базы данных, в которых содержатся сведения, составляющие государственную тайну, государственной регистрации не подлежат.

Правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы или базы данных, использовать **знак охраны авторского права**, состоящий из трех элементов:

- буквы С в окружности** или в круглых скобках ©;
- наименования (имени)** правообладателя;
- года первого выпуска** программы в свет.

**Авторские права на все виды программ для ЭВМ
охраняются так же, как авторские права на
произведения литературы.**

Личные права автора на программу или базу данных
охраняются бессрочно.

Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без разрешения автора и без выплаты дополнительного вознаграждения:

- 1) внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя ;**
- 2) изготавливать копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей;**
- 3) изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов любого элемента программы для ЭВМ ;**
- 4) воспроизвести и преобразовать объектный код, если это необходимо для достижения взаимодействию с другими программами;**

Заявка на регистрацию программы для ЭВМ или базы данных должна содержать:

- заявление о государственной регистрации** программы для ЭВМ или базы данных с указанием правообладателя, а также автора и места жительства или места нахождения каждого из них;
- депонируемые материалы**, идентифицирующие программу для ЭВМ или базу данных, включая реферат;
- документ, подтверждающий уплату государственной пошлины** в установленном размере или наличие оснований для освобождения от уплаты государственной пошлины, либо для уменьшения ее размера, либо для отсрочки ее уплаты.

Исключительное право изготовителя базы данных
возникает в момент завершения ее создания и **действует в течение пятнадцати лет**, считая с 1 января года, следующего за годом ее создания.

Исключительное право изготовителя базы данных, обнародованной в указанный период, действует **в течение пятнадцати лет**, считая с 1 января года, следующего за годом ее обнародования.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ АВТОРСКИХ ПРАВ

1. Техническими средствами защиты авторских прав признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения.
2. В отношении произведений **не допускается:**
 - 1) осуществление без разрешения автора или иного правообладателя действий, направленных на то, чтобы **удалить ограничения использования произведения**, установленные путем применения технических средств защиты авторских прав;

- 2) изготавление, распространение, сдача в прокат,**
предоставление во временное безвозмездное
пользование, импорт, реклама любой технологии, любого
технического устройства или их компонентов,
использование таких технических средств в целях
получения прибыли либо оказание соответствующих услуг,
если в результате таких действий становится
невозможным использование технических средств
защиты авторских прав либо эти технические средства не
смогут обеспечить надлежащую защиту указанных прав.
3. В случае нарушения этих положений **автор вправе**
требовать по своему выбору от нарушителя **возмещения**
убытков или выплаты компенсации.

ОХРАНА ТОПОЛОГИИ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

Топология - это зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы (ИМС) и связей между ними.

Автору топологии интегральной микросхемы, принадлежат следующие **интеллектуальные права**:

1) **исключительное право;**

2) **право авторства.**

**Предоставляемая правовая охрана распространяется
только на оригинальную топологию.**

**Оригинальной является топология, созданная в результате
творческой деятельности автора.**

**Автором топологии признается физическое лицо, в
результате творческой деятельности которого эта
топология была создана.**

**Граждане, создавшие топологию интегральной микросхемы
совместным творческим трудом, признаются соавторами.**

Топология, содержащая сведения, **составляющие государственную тайну**, государственной регистрации не подлежит.

Автору принадлежит **исключительное право** использовать эту топологию по своему усмотрению, в частности путем **изготовления и распространения ИМС с такой топологией**, включая право запрещать использование этой топологии другим лицам без соответствующего разрешения.

Правообладатель в течение срока действия исключительного права на топологию интегральной микросхемы **может** по своему желанию **зарегистрировать топологию** в федеральном органе исполнительной власти по интеллектуальной собственности.

Заявка на регистрацию должна относиться к одной топологии и содержать:

- 1) заявление о государственной регистрации топологии** с указанием лица, на имя которого испрашивается государственная регистрация, а также автора, если он не отказался быть упомянутым в качестве такового, места жительства или места нахождения каждого из них, даты первого использования топологии, если оно имело место;
- 2) депонируемые материалы**, идентифицирующие топологию, включая реферат;
- 3) документ, подтверждающий уплату пошлины** в установленном размере либо основания для освобождения от уплаты пошлины, или для уменьшения ее размера, или для отсрочки ее уплаты.

Правообладателю принадлежит **исключительное право использования топологии** любым не противоречащим закону способом (исключительное право на топологию).

Использованием топологии признаются действия, направленные на извлечение прибыли, в частности:

- 1) **воспроизведение топологии** в целом или частично путем включения в интегральную микросхему либо иным образом, за исключением воспроизведения только той части топологии, которая не является оригинальной;
- 2) **ввоз на территорию РФ, продажа и иное введение в гражданский оборот топологии**, или интегральной микросхемы, в которую включена эта топология, или изделия,ключающего в себя такую интегральную микросхему.

Правообладатель для оповещения о своем исключительном праве на топологию **вправе использовать знак охраны**, который помещается на топологии, а также на изделиях, содержащих такую топологию, и состоит из:

выделенной прописной буквы "T" ("T", [T], T*, буквы "T" в окружности, или буквы "T" в квадрате),

даты начала срока действия исключительного права на топологию

и информации, позволяющей идентифицировать правообладателя.

Право автора на топологию является неотъемлемым личным правом и охраняется законом бессрочно.

Исключительное право на использование топологии действует в течении десяти лет.

Автор топологии и иной правообладатель вправе требовать:
признания прав;
возмещения причиненных убытков.

За защитой своего права автор может обратиться в суд
(арбитражный или третейский).

Автор может требовать правовую охрану топологии в зарубежных странах.

Если международным договором РФ установлены иные правила, чем те, которые содержатся в настоящем Законе, то применяются правила международного договора.

Топология, созданная работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, признается служебной топологией.

Право авторства на служебную топологию принадлежит работнику.

Исключительное право на служебную топологию принадлежит работодателю, если договором между ним и работником не предусмотрено иное.

В случае, когда топология создана при выполнении **договора подряда** либо договора на выполнение НИОКР, которые прямо не предусматривали ее создание, **исключительное право на такую топологию принадлежит исполнителю**.

В случае, когда топология создана **по договору**, предметом которого было ее создание, **исключительное право на такую топологию принадлежит заказчику**.

10.2. ОБЪЕКТЫ ПАТЕНТНЫХ ПРАВ

Объектами патентных прав являются результаты интеллектуальной деятельности в научно-технической сфере, отвечающие требованиям к изобретениям и полезным моделям, и результаты интеллектуальной деятельности в сфере художественного конструирования, отвечающие установленным требованиям к промышленным образцам.

На изобретения, содержащие сведения, составляющие ГТ распространяются специальные правилами статей 1401 - 1405 настоящего Кодекса и изданными в соответствии с ними иными правовыми актами.

Не могут быть объектами патентных прав:

- способы клонирования человека;**
- способы модификации генетической целостности клеток зародышевой линии человека;**
- использование человеческих эмбрионов в промышленных и коммерческих целях;**
- иные решения, противоречащие общественным интересам, принципам гуманности и морали.**

В качестве изобретения охраняется техническое решение в **любой области, относящееся к продукту** (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) **или способу** (процессу осуществления действий над материальным объектом с помощью материальных средств).

Кодекс регулирует **имущественные**, а также **личные неимущественные отношения**, возникающие в связи с созданием, правовой охраной и использованием

изобретений,

полезных моделей (конструкторское выполнение) и

промышленных образцов (внешний вид).

Исключительное право на изобретение, полезную модель или промышленный образец признается и охраняется **при условии их государственной регистрации**, на основании которой федеральный орган исполнительной власти по интеллектуальной собственности выдает **патент на изобретение, полезную модель или промышленный образец.**

Изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо.

Изобретение является новым, если оно не известно из уровня техники.

Изобретение имеет изобретательский уровень, если для специалиста оно явным образом не следует из уровня техники

Изобретение является промышленно применимым, если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

Срок действия исключительного права на изобретение, полезную модель, промышленный образец и удостоверяющего это право патента исчисляется со дня подачи заявки на выдачу патента и составляет:

двадцать лет - для изобретений;

десять лет - для полезных моделей;

пятнадцать лет - для промышленных образцов.

Не являются изобретениями:

- 1) открытия;
- 2) научные теории и математические методы;
- 3) решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей;
- 4) правила и методы игр, интеллектуальной или хозяйственной деятельности;
- 5) программы для ЭВМ;
- 6) решения, заключающиеся только в представлении информации.

Не предоставляется правовая охрана в качестве изобретения:

- 1) сортам растений, породам животных и биологическим способам их получения, за исключением микробиологических способов и продуктов, полученных такими способами;
- 2) топологиям интегральных микросхем.

Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Право на получение патента, созданного работником в связи с выполнением им своих служебных обязанностей или полученным от работодателя заданием, принадлежит работодателю.

При этом **автор имеет право на вознаграждение**, соразмерное выгоде, которая получена работодателем или могла бы быть им получена.

Вознаграждение выплачивается в размере и на условиях, определяемых на основе соглашения между ними.

Патентообладателю принадлежит исключительное право на использование охраняемых патентом изобретения, полезной модели или промышленного образца по своему усмотрению.

Нарушением исключительного права патентообладателя признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный продукта, содержащего запатентованное изобретение.

Правительство РФ имеет право в интересах обороны и безопасности разрешить использование изобретения, полезной модели или промышленного образца без согласия патентообладателя с уведомлением его об этом в кратчайший срок и с выплатой ему соразмерной компенсации.

На изобретения, содержащие сведения, составляющие ГТ распространяются положения раздела «**Особенности правовой охраны и использования секретных изобретений**» настоящего Кодекса.

Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, **правовая охрана не предоставляется**.

В качестве полезной модели охраняется техническое решение, относящееся к устройству.

Полезной модели предоставляется правовая охрана, если **она является новой и промышленно применимой.**

В качестве промышленного образца охраняется художественно-конструкторское решение изделия промышленного или кустарно-ремесленного производства, определяющее его внешний вид.

Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным.

Заявка на изобретение должна содержать:

- 1) заявление о выдаче патента** с указанием автора изобретения и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;
- 2) описание изобретения**, раскрывающее его с полнотой, достаточной для осуществления;
- 3) формулу изобретения**, выражающую его сущность и полностью основанную на его описании;
- 4) чертежи и иные материалы**, если они необходимы для понимания сущности изобретения;
- 5) реферат.**

Заявка на полезную модель должна содержать:

- 1) заявление о выдаче патента** с указанием автора полезной модели и лица, на имя которого испрашивается патент, а также места жительства или места нахождения каждого из них;
- 2) описание полезной модели**, раскрывающее ее с полнотой, достаточной для осуществления;
- 3) формулу полезной модели**, выражющую ее сущность и полностью основанную на ее описании;
- 4) чертежи**, если они необходимы для понимания сущности полезной модели;
- 5) реферат.**

Заявка на промышленный образец должна содержать:

- 1) заявление о выдаче патента с указанием автора промышленного образца и лица, на имя которого спрашивается патент, а также места жительства или места нахождения каждого из них;**
- 2) комплект изображений изделия, дающих полное детальное представление о внешнем виде изделия;**
- 3) чертеж общего вида изделия, эргономическую схему, конфекционную карту (карту изготовления), если они необходимы для раскрытия сущности промышленного образца;**
- 4) описание промышленного образца;**
- 5) перечень существенных признаков промышленного образца.**

Экспертиза заявки на изобретение по существу включает:

- информационный поиск** в отношении заявленного изобретения для определения уровня техники, по сравнению с которым будет осуществляться оценка новизны и изобретательского уровня изобретения;
- проверку соответствия** заявленного изобретения условиям патентоспособности.

По истечении **шести месяцев** со дня начала экспертизы федеральный орган исполнительной власти по интеллектуальной собственности направляет заявителю отчет об информационном поиске.

На основании решения о выдаче патента на изобретение, полезную модель или промышленный образец федеральный орган вносит изобретение, полезную модель или промышленный образец в соответствующий государственный реестр:

Государственный реестр изобретений РФ,

Государственный реестр полезных моделей РФ,

Государственный реестр промышленных образцов РФ

и выдает патент

на изобретение, полезную модель или промышленный образец.

Публикация сведений о выдаче патента

Федеральный орган исполнительной власти по интеллектуальной собственности **публикует в официальном бюллете**не сведения о выдаче патента на изобретение, полезную модель или промышленный образец, включающие

- имя автора** (если автор не отказался быть упомянутым в качестве такового)
- имя или наименование патентообладателя,**
- название и формулу изобретения** или полезной модели либо перечень существенных признаков промышленного образца и его изображение.

Нарушением исключительного права патентообладателя признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный продукта, содержащего запатентованное изобретение.

Присвоение авторства, принуждение к соавторству, незаконное разглашение сведений об объекте промышленной собственности влекут за собой уголовную ответственность в соответствии с законодательством РФ.

Патент на селекционное достижение удостоверяет приоритет селекционного достижения, авторство и исключительное право на селекционное достижение.

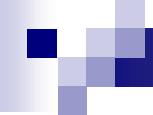
Срок действия исключительного права на селекционное достижение и удостоверяющего это право патента исчисляется со дня государственной регистрации селекционного достижения в Государственном реестре охраняемых селекционных достижений и **составляет тридцать лет.**

На сорта винограда, древесных декоративных, плодовых культур и лесных пород, в том числе их подвоев, срок действия исключительного права и удостоверяющего это право патента составляет **тридцать пять лет.**

УК статья 147. Нарушение изобретательских и патентных прав

1. Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб, - **наказываются**

штрафом в размере **от двухсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, **либо лишением свободы на срок до двух лет.**



2. Те же деяния, совершенные неоднократно либо группой лиц по предварительному сговору или организованной группой, - **наказываются**

штрафом в размере **от ста тысяч до трехсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо арестом на срок от четырех до шести месяцев, либо **лишением свободы на срок до пяти лет.**

Контрольные вопросы

- 1. Как осуществляется правовая охрана программ для ЭВМ и баз данных?**
- 2. Знак охраны топологии интегральных микросхем.**
- 3. Назовите объекты патентных прав.**
- 4. Срок действия исключительного права на изобретение, полезную модель, промышленный образец.**
- 5. В каком случае разрешается использование изобретения, полезной модели или промышленного образца без согласия патентообладателя?**
- 6. Срок действия исключительного права на селекционное достижение .**
- 7. Ответственность за нарушение изобретательских и патентных прав.**

Организационное и правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 10.2

- 1. Как осуществляется правовая охрана программ для ЭВМ и баз данных?**
- 2. Знак охраны топологии интегральных микросхем.**
- 3. Назовите объекты патентных прав.**
- 4. Срок действия исключительного права на изобретение, полезную модель, промышленный образец.**
- 5. В каком случае разрешается использование изобретения, полезной модели или промышленного образца без согласия патентообладателя?**
- 6. Срок действия исключительного права на селекционное достижение .**
- 7. Ответственность за нарушение изобретательских и патентных прав.**

10.3. ПРАВО НА ОИС В КОММЕРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Право на секрет производства (ноу-хау)

Секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Обладателю секрета производства принадлежит исключительное право его использования, в том числе при изготовлении изделий и реализации экономических и организационных решений.

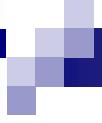
Лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета производства, приобретает самостоятельное исключительное право на этот секрет производства.

Исключительное право на секрет производства действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание.

С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей.

Нарушитель исключительного права на секрет производства, (лицо, которое неправомерно получило сведения, составляющие секрет производства, и разгласило или использовало эти сведения, а также лицо, обязанное сохранять конфиденциальность секрета производства), обязано возместить убытки, причиненные нарушением исключительного права на секрет производства.

Лицо, которое использовало секрет производства и не знало и не должно было знать о том, что его использование незаконно, в том числе в связи с тем, что оно получило доступ к секрету производства случайно или по ошибке, не несет ответственность.



Права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий

Закон регулирует отношения, возникающие в связи с регистрацией, правовой охраной и использованием

- фирменного наименования**
- товарных знаков,**
- знаков обслуживания**
- наименований мест происхождения товаров.**

Право на фирменное наименование

Юридическое лицо, являющееся коммерческой организацией, выступает в гражданском обороте под своим фирменным наименованием, которое определяется в его учредительных документах и включается в единый государственный реестр юридических лиц при государственной регистрации юридического лица.

Фирменное наименование юридического лица должно содержать указание на его организационно-правовую форму и собственно наименование юридического лица, которое не может состоять только из слов, обозначающих род деятельности.

В фирменное наименование юридического лица не могут включаться:

- 1) полные или сокращенные официальные наименования РФ, иностранных государств, а также слова, производные от таких наименований;**
- 2) полные или сокращенные официальные наименования федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления;**
- 3) полные или сокращенные наименования международных и межправительственных организаций;**
- 4) полные или сокращенные наименования общественных объединений;**
- 5) обозначения, противоречащие общественным интересам, а также принципам гуманности и морали.**

Юридическому лицу принадлежит **исключительное право использования своего фирменного наименования** в качестве средства индивидуализации (**исключительное право на фирменное наименование**), в том числе путем его указания на вывесках, бланках, в счетах и иной документации, в объявлениях и рекламе, на товарах или их упаковках.

Не допускается использование юридическим лицом фирменного наименования, тождественного фирменному наименованию другого юридического лица или сходного с ним до степени смешения, если указанные юридические лица осуществляют аналогичную деятельность и фирменное наименование второго юридического лица было включено в единый государственный реестр юридических лиц ранее, чем фирменное наименование первого юридического лица.

Юридическое лицо, нарушившее указанные правила, обязано по требованию правообладателя прекратить использование фирменного наименования, тождественного фирменному наименованию правообладателя или сходного с ним до степени смешения, в отношении видов деятельности, аналогичных видам деятельности, осуществляемых правообладателем, и возместить правообладателю причиненные убытки.

Исключительное право на фирменное наименование возникает со дня государственной регистрации юридического лица и прекращается в момент исключения фирменного наименования из единого государственного реестра юридических лиц в связи с прекращением деятельности юридического лица либо изменением его фирменного наименования.

Фирменное наименование или отдельные его элементы могут использоваться правообладателем в составе принадлежащего ему коммерческого обозначения.

Фирменное наименование, включенное в коммерческое обозначение, охраняется независимо от охраны коммерческого обозначения.

Фирменное наименование или отдельные его элементы могут быть использованы правообладателем в принадлежащем ему товарном знаке и знаке обслуживания.

Фирменное наименование, включенное в товарный знак или знак обслуживания, охраняется независимо от охраны товарного знака или знака обслуживания.

Право на товарный знак

На товарный знак, то есть на обозначение, служащее для индивидуализации товаров юридических лиц или индивидуальных предпринимателей, признается исключительное право, удостоверяемое свидетельством на товарный знак.

Правила настоящего Кодекса о товарных знаках соответственно применяются к знакам обслуживания, то есть к обозначениям, служащим для индивидуализации выполняемых юридическими лицами либо индивидуальными предпринимателями работ или оказываемых ими услуг.

Государственная регистрация товарного знака
осуществляется федеральным органом исполнительной
власти по интеллектуальной собственности в
**Государственном реестре товарных знаков и знаков
обслуживания РФ.**

**На товарный знак, зарегистрированный в Государственном
реестре товарных знаков, выдается свидетельство на
товарный знак.**

**Свидетельство на товарный знак удостоверяет приоритет
товарного знака и исключительное право на товарный
знак в отношении товаров, указанных в
свидетельстве.**

В качестве товарных знаков могут быть зарегистрированы словесные, изобразительные, объемные и другие обозначения или их комбинации в любом цвете или цветовом сочетании.

Исключительное право на товарный знак действует в течение десяти лет со дня подачи заявки на государственную регистрацию товарного знака в федеральный орган исполнительной власти по интеллектуальной собственности.

Срок действия исключительного права на товарный знак может быть продлен на десять лет по заявлению правообладателя, поданному в течение последнего года действия этого права.

Продление срока действия исключительного права на товарный знак возможно неограниченное число раз.

Не допускается государственная регистрация в качестве товарных знаков обозначений, не обладающих различительной способностью или состоящих только из элементов:

- 1) вошедших во всеобщее употребление для обозначения товаров определенного вида;**
- 2) являющихся общепринятыми символами и терминами;**
- 3) характеризующих товары, в том числе указывающих на их вид, качество, количество, свойство, назначение, ценность, а также на время, место и способ их производства или сбыта;**
- 4) представляющих собой форму товаров, которая определяется исключительно или главным образом свойством либо назначением товаров.**

Указанные элементы могут быть включены в товарный знак как неохраняемые элементы, если они не занимают в нем доминирующего положения.

Не допускается государственная регистрация в качестве товарных знаков обозначений, не обладающих различительной способностью или состоящих только из элементов, представляющих собой:

- 1) государственные гербы, флаги и другие государственные символы и знаки;**
- 2) сокращенные или полные наименования международных и межправительственных организаций, их гербы, флаги, другие символы и знаки;**
- 3) официальные контрольные, гарантийные или пробирные клейма, печати, награды и другие знаки отличия;**
- 4) обозначения, сходные до степени смешения с элементами, указанными в подпунктах 1 - 3 настоящего пункта.**

Такие элементы могут быть включены в товарный знак как неохраняемые элементы, если на это имеется согласие соответствующего компетентного органа.

Не допускается государственная регистрация в качестве товарных знаков обозначений, представляющих собой или содержащих элементы:

- 1) являющиеся ложными или способными ввести в заблуждение потребителя относительно товара либо его изготовителя;**
- 2) противоречащие общественным интересам, принципам гуманности и морали.**
- 3) тождественные или сходные с официальными наименованиями и изображениями особо ценных объектов культурного наследия народов РФ либо объектов всемирного культурного или природного наследия.**

Исключительное право на товарный знак может быть осуществлено для индивидуализации товаров, работ или услуг, путем размещения товарного знака:

- 1) на товарах**, в том числе на этикетках, упаковках товаров, которые производятся, предлагаются к продаже, продаются, демонстрируются на выставках и ярмарках или иным образом вводятся в гражданский оборот;
- 2) при выполнении работ**, оказании услуг;
- 3) на документации**, связанной с введением товаров в гражданский оборот;
- 4) в предложениях о продаже товаров**, о выполнении работ, об оказании услуг, а также в объявлениях, на вывесках и в рекламе;
- 5) в сети "Интернет"**, в том числе в доменном имени и при других способах адресации.

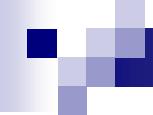
Правообладатель для оповещения о своем исключительном праве на товарный знак вправе использовать знак охраны, который помещается рядом с товарным знаком, состоит из **латинской буквы "R"** или латинской буквы "R" в окружности - ®, либо словесного обозначения "**товарный знак**" или "**зарегистрированный товарный знак**" и указывает на то, что применяемое обозначение является товарным знаком, охраняемым на территории РФ.

Заявка на товарный знак должна содержать:

- **заявление о государственной регистрации обозначения** в качестве товарного знака с указанием заявителя, его места жительства или места нахождения;
- **заявляемое обозначение;**
- **перечень товаров**, в отношении которых испрашивается государственная регистрация товарного знака;
- **описание заявляемого обозначения.**

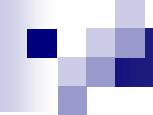
К заявке на товарный знак должны быть приложены:

- **документ, подтверждающий уплату пошлины** за подачу заявки в установленном размере;
- **устав коллектического знака**, если заявка подается на коллективный знак.



Товары, этикетки, упаковки товаров, на которых незаконно размещены товарный знак или сходное с ним до степени смешения обозначение, являются контрафактными.

Правообладатель вправе требовать изъятия из оборота и уничтожения за счет нарушителя контрафактных товаров, этикеток, упаковок товаров, на которых размещены незаконно используемый товарный знак или сходное с ним до степени смешения обозначение.



Правообладатель вправе требовать по своему
выбору от нарушителя **выплаты компенсации:**
в размере **от десяти тысяч до пяти миллионов**
рублей, определяемом по усмотрению суда;

в двукратном размере стоимости товаров, на
которых незаконно размещен товарный знак, или

в двукратном размере стоимости права
использования товарного знака, определяемой
исходя из цены, которая обычно взимается за
правомерное использование товарного знака.

Право на наименование места происхождения товара

Наименованием места происхождения товара, которому предоставляется правовая охрана, является обозначение, представляющее собой либо содержащее современное или историческое, официальное или неофициальное, полное или сокращенное наименование страны, городского или сельского поселения, местности или другого географического объекта.

На использование этого наименования может быть признано **исключительное право производителей такого товара.**

Исключительное право использования наименования места происхождения товара, предоставляется на основе его регистрации федеральным органом исполнительной власти по интеллектуальной собственности.

Использованием наименования места происхождения товара считается размещение этого наименования:

- на товарах**, этикетках, упаковках товаров, которые производятся, предлагаются к продаже, продаются, демонстрируются на выставках и ярмарках или иным образом вводятся в гражданский оборот;
- на бланках**, счетах, иной документации и в печатных изданиях;
- в предложениях о продаже товаров**, а также в объявлениях, на вывесках и в рекламе;
- в сети "Интернет"**, в том числе в доменном имени и при других способах адресации.

Товары, этикетки, упаковки товаров, на которых незаконно использованы наименования мест происхождения товаров или сходные с ними до степени смешения обозначения, являются контрафактными.

Обладатель свидетельства об исключительном праве на наименование места происхождения товара для оповещения о своем исключительном праве может помещать рядом с наименованием места происхождения товара знак охраны в виде словесного обозначения "зарегистрированное наименование места происхождения товара" или "зарегистрированное НМПТ", указывающий на то, что применяемое обозначение является наименованием места происхождения товара, зарегистрированным в РФ.

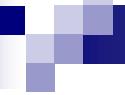
Свидетельство об исключительном праве на наименование места происхождения товара действует в течение десяти лет со дня подачи заявки на наименование места происхождения товара.

Срок действия свидетельства об исключительном праве на наименование места происхождения товара **может быть продлен** по заявлению обладателя свидетельства.

Срок действия свидетельства продлевается каждый раз на десять лет.

**Правообладатель вправе требовать по своему
выбору от нарушителя вместо возмещения
убытков выплаты компенсации:**

- в размере **от десяти тысяч до пяти миллионов рублей**, определяемом по усмотрению суда исходя из характера нарушения;
- в **двукратном размере стоимости товаров**, на которых незаконно размещено наименование места происхождения товара.



Право использования результатов интеллектуальной деятельности в составе единой технологии

Единой технологией признается выраженный в объективной форме результат научно-технической деятельности, который включает в том или ином сочетании изобретения, полезные модели, промышленные образцы, программы для ЭВМ или другие результаты интеллектуальной деятельности, подлежащие правовой охране, и может служить технологической основой определенной практической деятельности в гражданской или военной сфере (единая технология).

В состав единой технологии могут входить также результаты интеллектуальной деятельности, не подлежащие правовой охране, в том числе технические данные, другая информация.

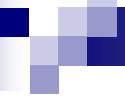
Право использовать результаты интеллектуальной деятельности в составе единой технологии как в составе сложного объекта принадлежит лицу, организовавшему создание единой технологии (право на технологию) на основании договоров с обладателями исключительных прав на результаты интеллектуальной деятельности, входящие в состав единой технологии.

В состав единой технологии могут входить также охраняемые результаты интеллектуальной деятельности, созданные самим лицом, организовавшим ее создание.

Лицо, которому принадлежит право на технологию, обязано
незамедлительно принимать меры для признания за ним
и получения прав на результаты интеллектуальной
деятельности, входящие в состав единой технологии-
-подавать заявки на выдачу патентов, на
государственную регистрацию результатов
интеллектуальной деятельности,
-вводить в отношении соответствующей информации
режим сохранения тайны,
-заключать договоры об отчуждении исключительных
прав и лицензионные договоры с обладателями
исключительных прав на соответствующие
результаты интеллектуальной деятельности,
входящие в состав единой технологии,
-и принимать иные меры.

Контрольные вопросы

- 1. Правовая защита на секрет производства.**
- 2. Правовая защита фирменного наименования.**
- 3. Знак охраны товарных знаков. Срок действия права на товарный знак.**
- 4. Правовая защита знаков обслуживания.**
- 5. Правовая защита наименований мест происхождения товаров.**
- 6. Срок действия исключительных прав на наименование мест происхождения товаров.**
- 7. Правовая защита использования результатов интеллектуальной деятельности в составе единой технологии .**



Организационно-правовое обеспечение информационной безопасности

Доцент кафедры БИТ

к.т.н.

Струков Владимир Ильич

Вопросы к разделу 10.3

- 1. Правовая защита на секрет производства.**
- 2. Правовая защита фирменного наименования.**
- 3. Знак охраны товарных знаков. Срок действия права на товарный знак.**
- 4. Правовая защита знаков обслуживания.**
- 5. Правовая защита наименований мест происхождения товаров.**
- 6. Срок действия исключительных прав на наименование мест происхождения товаров.**
- 7. Правовая защита использования результатов интеллектуальной деятельности в составе единой технологии .**

10.4. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В КОНКУРЕНТНОЙ БОРЬБЕ

Защита от недобросовестной рекламы

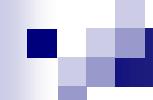
Закон “О рекламе” от 13 марта 2006 г. N 38-ФЗ

**реклама - информация, распространенная
любым способом, в любой форме и с
использованием любых средств,
адресованная неопределенному кругу лиц и
направленная на привлечение внимания к
объекту рекламирования, формирование
или поддержание интереса к нему и его
продвижение на рынке.**

Закон определяет **надлежащую** и **ненадлежащую** рекламу, которая соответственно соответствует и не соответствует требованиям законодательства.

Надлежащая реклама отвечает признакам **добросовестности** и **достоверности**.

Недобросовестная и **недостоверная** реклама не допускаются.



Недобросовестная реклама:

-содержит некорректные сравнения

рекламируемого товара с находящимися в обороте товарами других изготовителей;

-порочит честь, достоинство или деловую репутацию конкурента;

-представляет собой рекламу товара, реклама которого запрещена;

-является актом недобросовестной конкуренции
в соответствии с антимонопольным законодательством.



Недостоверная реклама содержит не соответствующие действительности сведения:

- о преимуществах рекламируемого товара перед товарами других изготовителей;
- о любых характеристиках товара, в том числе о его составе, дате изготовления, назначении и т.д.;
- об ассортименте и о комплектации товаров;
- о стоимости или цене товара;

- об условиях доставки, обмена товара;
- о гарантийных обязательствах изготовителя или продавца товара;
- об исключительных правах на результаты интеллектуальной деятельности;
- о правах на использование официальных государственных символов;
- о фактическом размере спроса на рекламируемый товар;

- об официальном или общественном признании, о получении медалей, призов, дипломов или иных наград;
- о его одобрении физическими или юридическими лицами;
- о результатах исследований и испытаний;
- о предоставлении дополнительных прав или преимуществ приобретателю рекламируемого товара;
- об объеме производства или продажи рекламируемого товара;

- о правилах и сроках проведения стимулирующей лотереи, конкурса, игры или иного подобного мероприятия;
- о правилах и сроках проведения основанных на риске игр, пари;
- об источнике информации, подлежащей раскрытию в соответствии с федеральными законами;
- об изготовителе или о продавце рекламируемого товара.



Реклама не должна:

- побуждать к совершению противоправных действий;
- призывать к насилию и жестокости;
- иметь сходство с дорожными знаками или угрожать безопасности движения транспорта;
- формировать негативное отношение к лицам, не пользующимся рекламируемыми товарами, или осуждать таких лиц.



В рекламе не допускаются:

- использование иностранных слов и выражений, которые могут привести к искажению смысла информации;
- указание на то, что объект рекламирования одобряется органами государственной власти;
- демонстрация процессов курения и потребления алкогольной продукции и пива;



- использование образов медицинских и фармацевтических работников;
- указание на то, что рекламируемый товар произведен с использованием тканей эмбриона человека;
- указание на лечебные свойства за исключением такого указания в рекламе лекарственных средств и медицинских услуг;
- использование бранных слов, непристойных и оскорбительных образов.



Не допускается

- **реклама**, в которой отсутствует существенная информация о рекламируемом товаре, об условиях его приобретения или использования, если при этом вводятся в заблуждение потребители рекламы.
- **использование** в радио-, теле-, видео-, аудио- и кинопродукции распространение **скрытой рекламы**, то есть рекламы, которая оказывает не осознаваемое потребителями воздействие на их сознание, в том числе такое воздействие путем использования специальных видеовставок (двойной звукозаписи) и иными способами.
- **размещение рекламы** в учебниках, предназначенных для обучения детей, школьных дневниках и тетрадях.

**В целях защиты несовершеннолетних в рекламе
не допускаются:**

- дискредитация** родителей и воспитателей;
- побуждение** несовершеннолетних к тому, чтобы они убедили родителей или других лиц приобрести рекламируемый товар;
- создание** у несовершеннолетних искаженного представления о доступности товара для семьи с любым уровнем достатка;
- показ** несовершеннолетних в опасных ситуациях;

- создание у несовершеннолетних впечатления, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками;
- формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром;
- преуменьшение уровня необходимых для использования рекламируемого товара навыков;
- формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью.

- товаров, производство которых запрещено законодательством РФ;
- наркотических средств, психотропных веществ;
- взрывчатых веществ и материалов, за исключением пиротехнических изделий;

- органов и тканей человека в качестве объектов купли-продажи;
- товаров, подлежащих государственной регистрации, в случае отсутствия такой регистрации;
- товаров, подлежащих обязательной сертификации в случае отсутствия такой сертификации;
- товаров, на производство и реализацию которых требуется получение лицензий, в случае отсутствия таких разрешений.

Правила прерывания теле- и радиопередач рекламой (ст. 14 и 15).

Не допускается прерывать рекламой и совмещать с
рекламой способом "бегущей строки "
религиозные телепередачи и

**телепередачи продолжительностью менее чем
пятнадцать минут.**

**В ст.16 и 17 закона закреплены нормы
размещения рекламы в печатных изданиях.**

Реклама в изданиях не рекламного характера не
должна превышать 40% объема и
сопровождаться пометками «реклама» или «на
правах рекламы».

В законе отдельно выделены разделы, касающиеся рекламы отдельных товаров, например: алкогольной продукции, табачных изделий, лекарственных средств, оружия, ценных бумаг.

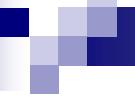
Реклама алкогольной продукции должна сопровождаться предупреждением о вреде ее чрезмерного потребления.

Реклама табака и табачных изделий должна сопровождаться предупреждением о вреде курения.

Такому предупреждению должно быть отведено не менее чем 10% рекламной площади.

Реклама алкогольной продукции не должна размещаться:

- **на первой и последней полосах** газет, а также на первой и последней страницах и обложках журналов;
- **в предназначенных для несовершеннолетних** печатных изданиях, аудио- и видеопродукции;
- **в теле- и радиопрограммах**, при кино- и видеообслуживании;
- **на всех видах транспортных** средств общего пользования;



Реклама пива и напитков, изготавливаемых на его основе, не должна размещаться

- **в телепрограммах** с 7 до 22 часов местного времени и в радиопрограммах с 9 до 24 часов местного времени
- **при кино- и видеообслуживании** с 7 до 20 часов местного времени

Реклама табака, табачных изделий не должна размещаться

- **в теле- и радиопрограммах, при кино- и видеообслуживании**

Реклама биологически активных добавок и пищевых добавок не должна:

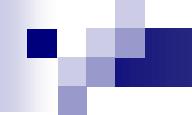
- создавать впечатление о том, что они являются лекарственными средствами и (или) обладают лечебными свойствами;**
- содержать ссылки на конкретные случаи излечения людей, улучшения их состояния в результате применения таких добавок;**
- содержать выражение благодарности физическими лицами в связи с применением таких добавок;**
- побуждать к отказу от здорового питания.**

Таким образом, к ненадлежащей рекламе относится:

- **Недобросовестная реклама** – содержит **некорректные сравнения** рекламируемого товара с товарами других лиц, а также, может содержать образы или высказывания, порочащие честь, достоинство, деловую репутацию конкурентов.

Методами такой рекламы становятся дискредитация конкурентов, высказывания, порочащие граждан, не пользующихся данным товаром или услугой.

Пример некорректной рекламы, ролик рекламирующий лосьон "Клирасил". Было признано, что эта реклама "паразитирует" на подростковых комплексах.



- Недостоверная реклама – содержит **сведения**, которые не соответствуют действительности.

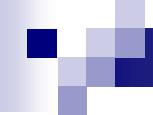
К таким сведениям относятся: характеристики товара, состав и способ изготовления, место происхождения, знаки соответствия госстандартам, возможность приобретения товара в указанном объеме в период времени и в месте, стоимость товара на момент распространения рекламы, наличие у товара официальных наград, призов, дипломов, использование терминов в превосходной степени (лучший, абсолютный, единственный).

Неэтическая реклама - содержит текстовую, зрительную или звуковую информацию, нарушающую общепринятые нормы гуманности и морали, путем употребления оскорбительных слов и выражений, а также образов в отношении расы, национальности, социальной категории, возрастной группы, пола, языка или профессии, а также религиозных, философских, политических и иных убеждений физических лиц.

Также неэтической является реклама, порочащая произведения искусства, составляющие национальное или мировое культурное достояние.

Скрытая реклама - реклама, которая потребителем как таковая не осознается.

Рекламный посыл может реализоваться в **журналистской статье** (джинса), в **двойной звукозаписи**, небольшой вставке в видеоматериал. Наиболее часто скрытая реклама фигурирует на ТВ (**демонстрации** каких либо марок товара (брендов) в художественных фильмах), а также в прессе, когда не всегда возможно доказать, что стало причиной написания статьи - **положительное впечатление от фирмы или товара** или **рекламный заказ** (в этом случае должна быть надпись: «**на правах рекламы**» или значек, обозначающий, что это реклама).



- **Заведомо ложная реклама** - реклама, с помощью которой

рекламодатель,

рекламопроизводитель или

рекламораспространитель

умышленно вводит в заблуждение
потребителя рекламы.

**Контроль в области рекламы осуществляется
федеральный антимонопольный орган.**

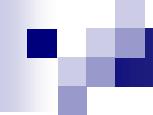
**Таким органом в настоящее время является
Федеральная антимонопольная служба (ФАС).**

Суммы штрафов за нарушение законодательства о рекламе зачисляются в бюджеты РФ в следующем порядке:

- 40 % в федеральный бюджет;
- 60 % в бюджет субъекта РФ, на территории которого зарегистрированы юридическое лицо допустившее нарушение законодательства о рекламе.

Фас осуществляет контроль за соблюдением законодательства о рекламе, в том числе:

- предупреждает, выявляет и пресекает нарушения физическими или юридическими лицами законодательства РФ о рекламе;**
- возбуждает и рассматривает дела по признакам нарушения законодательства РФ о рекламе.**



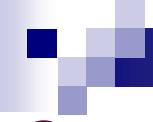
В статье 35 указаны обязанности антимонопольного органа по соблюдению коммерческой, служебной и иной охраняемой законом тайны.

Сведения, составляющие коммерческую, служебную и иную охраняемую законом тайну и полученные антимонопольным органом при осуществлении своих полномочий, не подлежат разглашению, за исключением предусмотренных федеральным законом случаев.



Разглашение сотрудниками антимонопольного органа сведений, составляющих **коммерческую, служебную и иную тайну**, влечет за собой ответственность в соответствии с законодательством РФ.

Убытки, причиненные таким разглашением, подлежат возмещению в соответствии с гражданским законодательством.



Ответственность за нарушение закона

-прекращение рекламы

- осуществление контррекламы

-уплата административного штрафа от 40 тыс. до 500 тыс. руб.

-возмещение убытков, морального и репутационного вреда

Зашита от недобросовестной конкуренции

Законы:

**“О конкуренции и ограничении
монополистической деятельности”, (Ред. от
9.10.2002 г №122-ФЗ)**

“О защите конкуренции” от 26.07.2006г. N135-ФЗ

**направлены на пресечение монополистической
деятельности и недобросовестной конкуренции.**

**Законом запрещается как недобросовестная
конкуренция:**

- распространение ложных, неточных или искаженных сведений**, которые могут причинить убытки хозяйствующему субъекту либо нанести ущерб его деловой репутации;
- введение в заблуждение в отношении характера, способа и места производства, потребительских свойств, качества и количества товара или в отношении его производителей;**

- некорректное сравнение хозяйствующим субъектом производимых или реализуемых им товаров с товарами, производимыми или реализуемыми другими хозяйствующими субъектами;
- продажа, обмен или иное введение в оборот товара, если при этом незаконно использовались результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, средства индивидуализации продукции, работ, услуг;
- незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну.

Контрольные вопросы

- 1. Каким законом регулируется рекламная информация?**
- 2. Каким признакам отвечает надлежащая реклама?**
- 3. Чем характерна недобросовестная реклама?**
- 4. Какая реклама запрещена?**
- 5. Какие существуют ограничения по размещения рекламы в печатных изданиях?**
- 6. Как регулируются прерывания теле- и радиопередач рекламой?**
- 7. Какой орган осуществляет контроль в области рекламы?**