

# **Организационное и правовое обеспечение информационной безопасности**

**Доценты кафедры БИТ**

**Струков Владимир Ильич**  
**Некрасов Алексей Валентинович**

# **ВВЕДЕНИЕ**

## **Цель, задачи и содержание курса**

### **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.

## **Объект защиты**

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

- персонал,
- документы,
- технические средства.

## **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 (Модуль 1)**

- 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**

**В Модуле 1 (сентябрь-октябрь) предусмотрены лекционные и практические занятия (компьютерные тесты).**

**По окончании всего курса у студентов бакалавриата – диф. зачет, у студентов специалитета – экзамен.**

## **Учебная и учебно-методическая литература**

1. Белов Е.Б., Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности: учебное пособие. – М.: Издательский центр «Академия», 2020 – 336 с.
2. Стрельцов А.А., Пожарский В.Н., Минаев В.А., Тарапанова Е.А., Фролов Д.Б., Скрыль С.В., Сычев А.М., Коробец Б.Н., Вайц Е.В., Грачёва Ю.В., Астрахов А.В. Организационно-правовое обеспечение информационной безопасности: учебник. – М.: МГТУ им. Баумана, 2018. – 291 с.
3. Ажмухамедов И.М., Князева О.М. Основы организационно-правового обеспечения информационной безопасности: учебное пособие. – Санкт-Петербург : Интермедиа, 2017. – 264 с.
4. Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие. – Санкт-Петербург: НИУ ИТМО, 2016. – 168 с.
5. Брюхомицкий, Ю.А. Безопасность информационных технологий: учебное пособие: часть 1. – Ростов-на-Дону: ЮФУ, 2020 – 171 с.
7. Струков В.И. Правовое обеспечение защиты информации. Учебно-методическое пособие: часть 1 (№ 4196) и часть 2 (№ 4196-2).
8. Струков В.И., Некрасов А.В. Презентации лекций по курсу ОиПОИБ Модуля 1.

## **Периодические издания**

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

## **Правовые документы**

- 1. Фед. зак. РФ “Об информации, информационных технологиях и о защите информации” от 27.07.2006 г. № 149-ФЗ.**
- 2. Фед. зак. РФ “О государственной тайне” от 21.07.1993 г. № 5485-1 (ред. 04.08.2023 г.).**
- 3. Фед. зак. РФ “О коммерческой тайне”, от 29.07.2004 г. № 98-ФЗ.**
- 4. Фед. зак. РФ “О персональных данных” от 27.07.2006 г. № 152-ФЗ.**
- 5. Фед. зак. РФ "Об электронной подписи" от 06.04.2011 г. № 63-ФЗ.**
- 6. Фед. зак. РФ “Об архивном деле в РФ” от 22.10.2004 г. № 125-ФЗ.**
- 7. Фед. зак. РФ “О федеральной фельдъегерской связи” от 17.12.1994г. № 67-ФЗ (ред. от 04.08.2023 г.).**
- 8. Гражданский кодекс РФ, Уголовный кодекс РФ и др. кодексы.**
- 9. Фед. зак. РФ “О лицензировании отдельных видов деятельности”, от 04.05.2011 г. № 99-ФЗ (ред. от 04.08.2023 г.).**

## **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 обычно 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 высших  
органов исполнительной власти  
субъектов РФ**

**Нормативные правовые акты  
федеральных органов  
исполнительной власти**

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

**Правовые акты органов местного самоуправления**

**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 (на ношение оружия, управление транспортным средством и т.д.), 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 составляющие его отрасли.

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);**

- **гражданко-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 юридических принципов и норм, регулирующих отношения между государствами.

В широком смысле выделяются 3 основных направления:

**- международное публичное право**

особая правовая система, регулирующая отношения между государствами, созданными ими международными организациями и некоторыми другими субъектами международного общения.

**- международное частное право**

совокупность норм внутригосударственного законодательства, международных договоров и обычаев, которые регулируют гражданско-правовые, трудовые и иные отношения, осложнённые иностранным элементом.

**- наднациональное право**

форма международного права, при которой государства идут на сознательное ограничение некоторых своих прав и делегирование некоторых полномочий наднациональным органам.

### **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 28.06.1993 г. № 966.*

**Гражданский кодекс РФ** (в 4-х частях, 1-я 1994 г., 2-я 1996 г., 3-я 2001 г., 4-я 2006 г.

**Закон РФ “Об информации, информатизации и защите информации”** принят в 1995 г. - утратил силу

(действующий закон **Об информации, информационных технологиях и о защите информации** от 27.07.2006 № 149-ФЗ

## 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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**

## **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 27.07.2006 г. № 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 электронной подписи (ЭП; ранее – электронная цифровая подпись, ЭЦП).**

**Электронная подпись – собственноручная подпись в электронном виде, которой можно подписывать документы.**

## **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);

**информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

**информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

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

- обладатель информации** – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
- доступ к информации** – возможность получения информации и ее использования;
- конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- предоставление информации** – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- распространение информации** – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

- электронное сообщение** – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;
- документированная информация** – зафиксированная на материальном носителе информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;
- электронный документ** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;
- 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 подписью, признается, равнозначным документу, подписенному 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 России),**

**Служба специальной связи и информации при Федеральной службе охраны РФ (Спецсвязь ФСО России),**

**Федеральная служба по техническому и экспортному контролю  
РФ (ФСТЭК России) (бывшая Государственная техническая  
комиссия при Президенте Российской Федерации  
(Гостехкомиссия России), ГТК),**

**Государственная фельдъегерская служба РФ (ГФС России),**

**Межведомственная комиссия по защите государственной тайны.**

**Требования о защите информации, содержащейся 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**

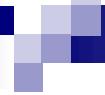
**Обладателем информации может быть физическое лицо, юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.**

**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 (в зависимости от порядка ее 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 27.07.2006 г. № 149-ФЗ и Указом Президента РФ “Об утверждении перечня сведений конфиденциального характера” от 06.03.1997 г. № 188

<b>Режим доступа</b>	<b>Вид режима</b>	<b>Состав сведений</b>
<b>Свободный доступ</b>	Общественного достояния	Научные открытия, рукописи и т.п.
	Массовой информации	Информация в СМИ, различные публикации и т.д.
	Исключительных прав	Результаты интеллектуальной деятельности
<b>Ограниченный доступ</b>	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,**
- секреты производства - «ноу-хау».**

Режим исключительных прав определен

**Гражданским кодексом РФ, часть 4, от 18.12.2006 г. № 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 27.12.1991 г.  
№ 2124-1.**

## **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 "Об утверждении перечня сведений конфиденциального характера" № 188 от 06.03.1997 г. 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 "Об утверждении перечня сведений конфиденциального характера" от 06.03.1997 г. № 188 утвержден перечень сведений конфиденциального характера:

**Коммерческая тайна** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

**Служебная тайна** – служебные сведения, которые не относятся к государственной тайне, доступ к которым ограничен органами государственной власти и федеральными органами исполнительной власти в соответствии с законодательством. Это информация о деятельности государственных органов власти и органов местного самоуправления, доступ к которой ограничен нормативно-правовыми актами государства, а также это сведения, которые поступают в вышеупомянутые органы на законном основании для исполнения служебных обязанностей.

**Профессиональная тайна**

**Персональные данные**

**Тайна следствия и судопроизводства**

**Сведения о защищаемых лицах и мерах государственной защиты**

**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**

**Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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.

## **Нормативно-правовыми документами в отношении защиты служебной тайны являются:**

**Закон РФ “О государственной гражданской службе Российской Федерации” от 27.07.2004 г. № 79-ФЗ.**

**Закон РФ “О прокуратуре РФ” от 17.01.1992 г. № 2202-1.**

**Закон РФ “О банках и банковской деятельности” от 02.12.1990 г. № 395-1.**

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

**Закон РФ “Об оперативно-розыскной деятельности” от 12.08.1995 г. № 144-ФЗ.**

**Закон РФ “О связи” от 07.07.2003 № 126-ФЗ.**

**Закон РФ “О коммерческой тайне” от 29.07.2004 г. № 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.**

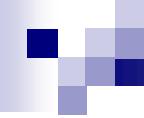
При этом получатель электронного сообщения вправе **установить отправителя электронного сообщения.**

**Единая система идентификации и аутентификации (ЕСИА)** была создана согласно Постановлению Правительства РФ от 28.11.2011 г. № 977 (ред. от 09.12.2013 г.) «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

ЕСИА – федеральная государственная информационная система, которая обеспечивает санкционированный доступ участников информационного взаимодействия в единой системе идентификации и аутентификации к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах.

Следует отметить, что в Законе “Об информации...” также имеются следующие 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 оперативно-розыскную деятельность (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 ОРД 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.**



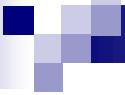
**3. Неисполнение организатором распространения информации в сети "Интернет" обязанности обеспечивать реализацию установленных в соответствии с ФЗ требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения уполномоченными государственными органами, осуществляющими ОРД 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 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351**

1. Установить, что:

а) подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу РФ, в том числе к международной компьютерной сети "Интернет" не допускается;



б) при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных в подпункте "а" настоящего пункта, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством РФ порядке сертификацию в ФСБ РФ и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю (ФСТЭК). Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;

- в) государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством РФ порядке сертификацию в ФСБ РФ и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;
- г) размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях. Финансирование расходов, связанных с размещением технических средств в указанных помещениях федеральных органов государственной власти, осуществляется в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете на содержание этих органов.

## **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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**

## **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 21.07.1993 г.  
№ 5485-1.**

**Закон регулирует отношения, связанные с:**

- отнесением сведений к государственной тайне (ГТ),**
- их рассекречиванием,**
- 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:**

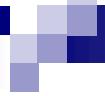
- **органы государственного управления;**
- **юридические лица**, независимо от их организационно-правовых форм деятельности и видов собственности;
- **граждане и должностные лица**, которые взяли на себя обязательство либо обязаны по своему статусу выполнять требования законодательства о государственной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

## **Перечень сведений, отнесенных к ГТ, утвержден**

**Указом Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30.11.1995 г. № 1203.**

**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 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» № 870 от 04.09.1995 г.**

**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:**

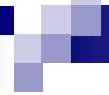
**ДСП – для служебного пользования.**

**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.



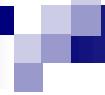
**На носители сведений, составляющих ГТ, наносятся реквизиты, включающие следующие данные:**

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

**На носителе 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 «Сведения, не подлежащие отнесению к государственной тайне и засекречиванию» закона о ГТ (которые раньше относились к ГТ).

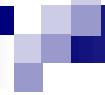
**Порядок засекречивания** сведений, составляющих ГТ, основан на трех принципах:

## **Принцип обоснованности**

заключается в установлении целесообразности

засекречивания сведений по экономическим

или иным критериям.



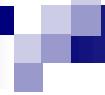
**Порядок засекречивания** сведений, составляющих ГТ, основан на трех принципах:

## **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. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию):

- 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.**

Обоснованность отнесения сведений к государственной тайне и их засекречивание заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов государства, общества и граждан.

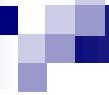
**Обоснование необходимости отнесения сведений к ГТ в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).**

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

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

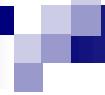
Указанный Перечень утверждается Президентом РФ, подлежит открытому опубликованию и пересматривается по мере необходимости.

**Перечень должностных лиц**, наделенных полномочиями по отнесению сведений к ГТ, утвержден распоряжением Президента РФ «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» от 16.05.2005 г. № 151-рп.



**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.**

Основания для рассекречивания сведений устанавливает статья 13 Закона РФ «О государственной тайне». К ним относятся:

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

Под рассекречиванием сведений и их носителей в названном Законе понимается: «снятие ранее введенных в предусмотренном настоящим Законом порядке ограничений на распространение сведений, составляющих ГТ, и на доступ к их носителям».

Порядок рассекречивания носителя сведений, составляющих ГТ, определяет статья 14 Закона РФ «О государственной тайне». Она устанавливает, что «носители сведений, составляющих ГТ, рассекречиваются не позднее сроков, установленных при их засекречивании». До истечения сроков засекречивания носители сведений, составляющих ГТ, подлежат рассекречиванию при изменении действующего в данном органе государственной власти, на предприятии, в учреждении и в организации развернутого перечня сведений, подлежащих засекречиванию, на основании которого они были засекречены.

Кроме того, руководители органов государственной власти, предприятий, учреждений и организаций имеют право осуществлять рассекречивание носителей сведений, необоснованно засекреченных подчиненными им должностными лицами.

**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,**
- **Министерство обороны (МО),**
- **Служба внешней разведки (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 "О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны" № 573 от 18.09.2006 г. установлен размер ежемесячной процентной надбавки к должностному окладу.

За работу со сведениями имеющими степень секретности устанавливается надбавка к должностному окладу:

**"ОВ" 50-75 %,**

**"СС" 30-50 %,**

**"С" 10-15 %** при оформлении допуска с проведением проверочных мероприятий,

**5-10 %** без проведения проверочных мероприятий.

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

**Первая – к сведениям «ОВ»**

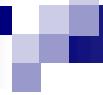
**Вторая – к сведениям «СС»**

**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.

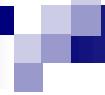
Сроки, обстоятельства и порядок переоформления допуска граждан к ГТ устанавливаются нормативными документами Правительством РФ.

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



**Особый порядок допуска к ГТ имеют, например:**

**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 21.1. Закона «О  
государственной тайне», которая определяет круг  
должностей, занимая которые лицо автоматически  
считается допущенным к гостайне без проведения  
проверочных мероприятий со стороны ФСБ, если по роду  
деятельности им требуется разрешение на работу с  
гостайной.**



## Особый порядок допуска к ГТ имеют

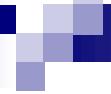
Указанные лица предупреждаются о неразглашении ГТ, ставшей им известной в связи с исполнением ими своих полномочий, и о привлечении их к ответственности в случае ее разглашения, о чем у них отбирается соответствующая расписка.

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



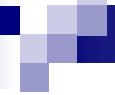
Должностное лицо или гражданин, допущенные к ГТ, могут быть временно **ограничены в следующих правах**:

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

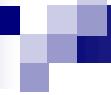


**Допуск должностного лица или гражданина к ГТ может быть прекращен по решению руководителя органа государственной власти, предприятия, учреждения или организации в случаях:**

- 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;**
- **прекращения 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**

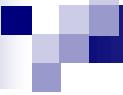
**экспертизы предприятия, учреждения и  
организации и**

**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**

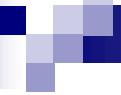
**Ответственность за организацию защиты сведений, составляющих ГТ, в органах государственной власти, на предприятиях, в учреждениях и организациях возлагается на их руководителей.**

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 совершенные гражданином РФ шпионаж, выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, доверенную лицу или ставшую известной ему по службе, работе, учебе или в иных случаях, предусмотренных законодательством РФ, переход на сторону противника либо оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности РФ, - **наказывается лишением свободы на срок от двенадцати до двадцати 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 и с ограничением свободы на срок до двух лет или **пожизненным лишением свободы**.



**Примечание 1. Под переходом на сторону противника в настоящей статье понимается участие лица в составе непосредственно противостоящих Российской Федерации сил (войск) иностранного государства, международной либо иностранной организации в вооруженном конфликте, военных действиях или иных действиях с применением вооружения и военной техники.**

**Примечание 2. Лицо, совершившее преступления, предусмотренные настоящей статьей, а также статьями 276 и 278 настоящего Кодекса, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления.**

## **Статья 276. Шпионаж**

**Передача, собирание, похищение или хранение** в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности Российской Федерации либо передача, собирание, похищение или хранение в целях передачи противнику сведений, которые могут быть использованы против Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов Российской Федерации, совершенные в условиях вооруженного конфликта, военных действий или иных действий с применением вооружения и военной техники с участием Российской Федерации, то есть шпионаж, если эти деяния совершены иностранным гражданином или лицом без гражданства, - **наказываются** лишением свободы на срок **от десяти до двадцати лет.**

## **Статья 283. Разглашение государственной тайны**

**Разглашение сведений, составляющих ГТ, лицом, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, если эти сведения стали достоянием других лиц, при отсутствии признаков преступлений, предусмотренных статьями 275 и 276 настоящего Кодекса, - 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 или без такового.**

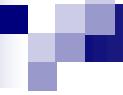
То же деяние, повлекшее по неосторожности **тяжкие последствия**, - наказываются лишением свободы на срок **от трех до семи лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

## Статья 284. Утрата документов, содержащих ГТ

**Нарушение лицом, имеющим допуск к ГТ, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, 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 с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.**

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

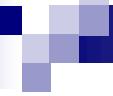
**Утрата документов** – это выход (в т.ч. и временный) документов из владения ответственного за их сохранность лица, которому они были доверены по службе или работе, являющийся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы стали или могли стать достоянием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



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

**ведомственный контроль,  
который осуществляют**

Органы государственной власти, наделенные в соответствии с настоящим Законом полномочиями по распоряжению сведениями, составляющими ГТ. Они обязаны контролировать эффективность защиты этих сведений во всех подчиненных и подведомственных им 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, который 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».** (По окончании рабочего дня, перед уходом, нужно убрать все с вашего рабочего места, а именно со стола (или другой поверхности)).
- 6. Создание службы безопасности фирмы.**
- 7. Использование технических средств защиты.**
- 8. Применение сертифицированных программных и аппаратных средств защиты информации (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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**

## **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 сбор информации фирмой о рынке, о партнерах и другой полезной информации, как правило, носит разведывательный характер.**

**Главным предметом разведки является КОММЕРЧЕСКАЯ ТАЙНА (КТ).**

**Принято различать:**

**конкурентную разведку** (синонимы: бизнес-разведка, деловая разведка, аналитическая разведка, экономическая разведка, маркетинговая разведка, коммерческая разведка) и

**промышленный шпионаж.**

**Отличие в первом случае заключается в соблюдении закона, а во втором – в нарушениях уголовного, авторского или любого другого права.**



**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 мошенничеств 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" от 11.03.1992 г. № 2487-1.**
- 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 базах данных (БД);**
- анализ годовых отчетов предприятий;**
- обратный инжиниринг** - исследование некоторого готового устройства или программы, а также документации на него с целью понять принцип его работы; например, чтобы обнаружить недокументированные возможности (в том числе программные закладки), сделать изменение или воспроизвести устройство, программу или иной объект с аналогичными функциями, но без прямого копирования. Обычно применяется когда создатель оригинального объекта не предоставил информации о структуре и способе создания (производства) объекта. Правообладатели таких объектов могут заявить, что проведение обратной разработки или использование ее результатов нарушает их исключительное право по закону об авторском праве и патентному законодательству.

**В настоящее время широко используется**

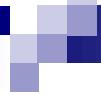
**конкурентная разведка через Интернет.**

**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.

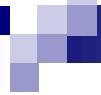
*В мире существуют тайные биржи, где продают промышленные секреты: например,*

*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" (утратил силу).**

**Затем в Законе РФ "Об информации, информатизации и защите информации" от 25.01.1995 г. (утратил силу, заменен Законом РФ "Об информации, информационных технологиях и о защите информации" от 27.06.2006 г. № 149-ФЗ),**

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

**в Законе РФ "О коммерческой тайне", от 29.07.2004 г. № 98-ФЗ**



## **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.**

## **2. Техническая информация:**

- научно-исследовательские проекты;
- конструкторская документация на продукцию;
- заявки на патенты;
- дизайн, передовые технологии и оборудование;
- программное обеспечение ЭВМ и информационный процесс (Информационный процесс - процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации.);
- химические формулы.

### **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»** (портрет клиента или аватар – усредненное описание человека, который будет покупать продукт) 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 целей 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** (научно-исследовательские и опытно-конструкторские работы – совокупность работ, направленных на получение новых знаний и их практическое применение при создании нового изделия или технологии).

Научно-исследовательские работы (НИР) – работы поискового, теоретического и экспериментального характера, выполняемые с целью определения технической возможности создания новой техники в определенные сроки, подразделяются на фундаментальные (получение новых знаний) и прикладные (применение новых знаний для решения конкретных задач) исследования.

Опытно-конструкторские работы (ОКР) и Технологические работы (ТР) – комплекс работ по разработке конструкторской и технологической документации на опытный образец изделия, изготовлению и испытаниям опытного образца изделия, выполняемых по техническому заданию.).

### **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, Санкт-Петербург, Тамбов, Нижний Новгород, Челябинск, Самара, Пермь), входящая в IGK Group.**

**За умеренную плату она представляет своим клиентам необходимую информацию.**

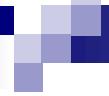
## **4.2. Защита коммерческой тайны**

**Отличие коммерческой тайны 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 может быть предложена трехуровневая система обозначения степени ее секретности:

**Коммерческая тайна – строго конфиденциально (КТ-СК)**

**Коммерческая тайна – конфиденциально (КТ-К)**

**Коммерческая тайна (КТ)**

Промежуточный гриф рекомендуется использовать

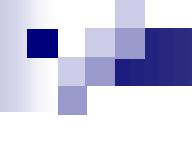
**Для внутреннего использования (ДВИ).**



## **Закон "О коммерческой тайне" от 29.07.2004 г. № 98-ФЗ**

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)

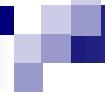


**КТ** – это научно-техническая, технологическая, производственная, финансово-экономическая информация в том числе составляющая секреты производства (ноу-хай), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа 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.

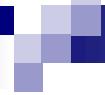
**Не могут составлять КТ (ст. 5) сведения:**

- 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;

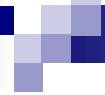


- 4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической обстановке и других факторах;
- 5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной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

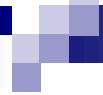


- 9) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- 10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- 11) сведения, недопустимость ограничения доступа к которым установлена иными федеральными законами.



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

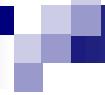
**Мотивированное требование** должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей КТ, и срок предоставления этой информации. (мотивированное – значит обоснованное).



**Режим коммерческой тайны является обязательным условием охраны конфиденциальности информации**

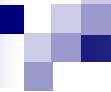
**Законом о КТ установлены требования, предъявляемые к режиму коммерческой тайны**

**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;**

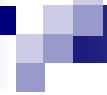
- 4) регулирование отношений по использованию информации, составляющей КТ, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров (контрагент - лицо или учреждение, берущее на себя известные обязательства по договору);**
- 5) нанесение на документы, содержащие 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.**

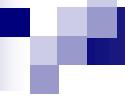
**1. Собирание сведений, составляющих коммерческую,**  
**налоговую или банковскую тайну, путем похищения**  
**документов, подкупа или угроз, а равно иным**  
**незаконным способом - наказывается штрафом в**  
**размере до восьмидесяти тысяч рублей или в**  
**размере заработной платы или иного дохода**  
**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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич**  
**Некрасов Алексей Валентинович**

## **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 договоры 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.**

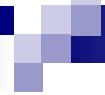
**Трудовой коллектив принимает на себя обязательство по соблюдению установленных на предприятии требований по защите КТ.**

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.**

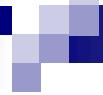
**Независимо от формы заключения договора (устная или письменная) подпись работника на приказе о приеме на работу подтверждает его согласие с условиями договора.**

**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 нем, 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 входящего и исходящего документа;
    - инвентарный учет;
    - номенклатуру дел, журналов и карточек;
    - контроль за местоположением документов.

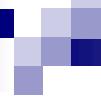


Корреспонденция с грифом “КТ” поступает в ОЗД, где она проверяется на наличие недостачи и регистрируется на карточках или в журнале.

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 вычислительной техники (ВТ).**

**На последнем листе каждого экземпляра проставляется количество отпечатанных экземпляров, фамилия исполнителя, машинистки (которая печатала документ) 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**

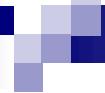
**ежеквартально – для документов, находящихся на исполнении;**

**ежегодно – для всех зарегистрированных документов.**

**Режимные документы**, находящиеся 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 порядка хранения и уничтожения документов;
- установление порядка обращения с документами.



## **Порядок хранения и уничтожения 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 записи 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**.

**Трудовой договор** – это соглашение между работодателем и работником, в котором определены права и взаимные обязанности сторон. Содержанием трудового договора являются взаимные права и обязанности и установлена ответственность при исполнении должностных инструкций.

**Должностная инструкция** – это внутренний организационно-распорядительный документ, содержащий конкретный перечень должностных обязанностей работника с учетом особенностей организации производства, труда и управления, а также его прав и ответственности.

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 (комерческой) 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** (По договору поручительства поручитель обязывается перед кредитором другого лица отвечать за исполнение последним его обязательства полностью или в части. Договор поручительства может быть заключен в обеспечение как денежных, так и неденежных обязательств, а также в обеспечение обязательства, которое возникнет в будущем.);
- **договор коммерческого представительства** (Коммерческим представителем является лицо, постоянно и самостоятельно представляющее от имени предпринимателей при заключении ими договоров в сфере предпринимательской деятельности);
- **агентский договор** (По агентскому договору одна сторона (агент) обязуется за вознаграждение совершать по поручению другой стороны (принципала) юридические и иные действия от своего имени, но за счет принципала либо от имени и за счет принципала.);

- **договор поручения или доверенности** (По договору поручения одна сторона (поверенный) обязуется совершить от имени и за счет другой стороны (доверителя) определенные юридические действия, может быть как бессрочным, так и срочным. Права и обязанности по сделке, совершенной поверенным, возникают непосредственно у доверителя. Полномочия поверенного в отношениях с третьими лицами оформляются с помощью особенного документа – доверенности, которую ему выдаёт доверитель. Доверенность – представляет собой, письменно оформленное и заверенное поручительство, которое одно лицо выдает другому для представительства и взаимодействия с другими физическими и юридическими лицами.);
- **договор о рекламных услугах** (представляет собой соглашение, по которому одна сторона по поручению другой стороны осуществляет рекламную кампанию какого-либо продукта.);
- **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 службу безопасности (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.**

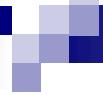
**Защита прав обладателя коммерческих секретов осуществляется способами, предусмотренными также ГК РФ и другими законами.**

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 компьютерных преступлений (КП) во всем мире составляют миллиарды долларов в год. Особенно страдают кредитно-финансовые учреждения.

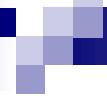
Кроме этих действий значительные потери возникают в результате распространения вредоносных программ - компьютерных вирусов, появившиеся начиная с 1987 г.

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 автоматизированных системах (АС).

### **1. Перехват информации:**

- по электромагнитному излучению** (излучения электронно-лучевые трубы (ЭЛТ) можно принимать на расстояниях до 1000 м.);
- по виброакустическому каналу** (таблетки, клопы, жучки, через несущие конструкции и проемы здания, стетоскоп);
- видеoperехват** (бинокль, фото- и видеокамеры);
- использование отходов информационного процесса** (физические - диски, 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. Вредоносные программы**

Вредоносная программа – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации.

Вредоносные программы могут быть классифицированы по:

- по вредоносной нагрузке;**
- по методу размножения.**

**По методу размножения** вредоносное ПО подразделяется на:

**Эксплойт** – теоретически безобидный набор данных (например, графический файл или сетевой пакет), некорректно воспринимаемый программой, работающей с такими данными. Здесь вред наносит не сам файл, а неадекватное поведение ПО с ошибкой, приводящее к уязвимости. Также эксплойтом называют программу для генерации подобных «отравленных» данных.

**Логическая бомба** – вредоносная часть компьютерной программы (полезной или нет), срабатывающая при определённом условии.

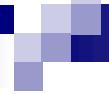
**Троянская программа** не имеет собственного механизма размножения и устанавливается «в придачу» к полезной или под видом полезной. Часто «в придачу» ставят ПО, которое не является истинно вредоносным, но является нежелательным – например, рекламным.

**Компьютерный вирус** размножается в пределах компьютера и через сменные диски. Размножение через сеть возможно, если пользователь сам выложит заражённый файл в сеть. Вирусы, в свою очередь, делятся:

- по типу заражаемых файлов (файловые, загрузочные, макро-, автозапускающиеся);
- по способу прикрепления к файлам (паразитирующие, «спутники» и перезаписывающие) и т.д.

**Сетевой червь** способен самостоятельно размножаться по сети. Делятся на IRC-черви (распространяются через IRC-каналы (чат-каналы, Internet Relay Chat), почтовые, размножающиеся с помощью эксплойтов ) и т.д.

Вредоносное ПО может образовывать цепочки: например, с помощью эксплойта (1) на компьютере жертвы развертывается загрузчик (2), устанавливающий из интернета червя-вирус (3-4) с логическими бомбами (5).

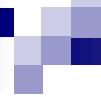


## 5. Использование специальных программных средств:

- “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 1996 г. 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 охраняемой законом компьютерной информации**, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - 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 до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

**2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности,-**  
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 ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

**3. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -**

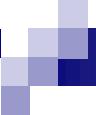
**наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.**

**4. Те же деяния, если они повлекли тяжкие последствия или создали угрозу их наступления, -**

**наказываются лишением свободы на срок до семи лет.**

**Примечание 1.** Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

**Примечание 2.** Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

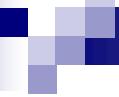


## **Статья 273. Создание, использование и распространение вредоносных компьютерных программ**

**1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок 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 совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.**

**3. Те же деяния, повлекшие по неосторожности тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок от трех до семи лет.**



## **Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей**

**1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -**  
**наказывается штрафом в размере до пятисот 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 ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.**

**2. То же деяние, если оно повлекло тяжкие последствия или создало угрозу их наступления, -**  
**наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.**



Целям защиты информации, обрабатываемой в АС служит  
**Закон РФ "Об электронной подписи" от 06.04.2011 г. № 63-ФЗ**

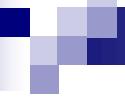
**ЭП** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

ЭП – собственноручная подпись в электронном виде, которой можно подписывать документы.

ЭП признается равнозначной собственноручной подписи лица на бумажном носителе, заверенном печатью.

## **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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**

## **Вопросы к подразделам 4.4 и 4.5**

- 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 11.03.1992 г. № 2487-1,  
«О безопасности» от 28.12.2010 г. № 390-ФЗ,  
«Об оружии» от 13.12.1996 г. № 150-ФЗ,  
«Об информации, информационных технологиях и о защите информации» от 27.13.2006 г. № 149-ФЗ,  
«О ведомственной охране» от 14.04.1999 г. № 77-ФЗ,  
ГК РФ и Трудовой Кодекс.

## **Постановления Правительства РФ:**

«Вопросы частной детективной (сыскной) и частной охранной деятельности» от 14.08.1992 г. № 587,  
«Об организации ведомственной охраны» от 12.07.2000 г. № 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», от 11.03.92 г. № 2487-1**

**Основные положения:**

Частная детективная и охранная деятельность **осуществляется физическими и юридическими лицами**, имеющими специальное разрешение (**лицензию**) (ст. 1), которая выдается **органом внутренних дел** (лица, занимающиеся частной детективной деятельностью, не вправе осуществлять оперативно–розыскные действия).

Согласно **Постановлению Правительства РФ “О лицензировании отдельных видов деятельности” от 04.05.2011 г. № 99-ФЗ** подлежат лицензированию (ст. 12):  
32) частная охранная деятельность;  
33) частная детективная (сыскная) деятельность.

Частная детективная и охранная деятельность осуществляется для сыска и охраны.

## **В целях сыска**

разрешается предоставление следующих

**8 видов услуг** (ст. 3):

**1) сбор сведений** по гражданским делам на договорной основе с участниками процесса;

**2) изучение рынка**, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;

**3) установление обстоятельств неправомерного использования** в предпринимательской деятельности фирменных знаков и наименований, недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;

**4) выяснение** биографических и других характеризующих личность данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов;

- 5) поиск без вести пропавших граждан;**
- 6) поиск утраченного имущества гражданами или предприятиями, учреждениями, организациями;**
- 7) 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 лицо, производящее дознание, следователя или суд, в чьем производстве находится уголовное дело;
- 8) поиск лица, являющегося должником** в соответствии с исполнительным документом, его имущества, а также поиск ребенка по исполнительному документу, содержащему требование об отобрании или о передаче ребенка, порядке общения с ребенком, требование о возвращении незаконно перемещенного в РФ или удерживаемого в РФ ребенка или об осуществлении в отношении такого ребенка прав доступа на основании международного договора РФ, на договорной основе с взыскателем.

## **В целях охраны**

разрешается предоставление следующих **7 видов услуг:**

- 1) защита жизни и здоровья граждан;**
- 2) охрана объектов и (или) имущества** (в том числе при его транспортировке), находящихся в собственности, во владении, в пользовании, хозяйственном ведении, оперативном управлении или доверительном управлении, за исключением объектов и (или) имущества, предусмотренных пунктом 7 настоящей части;
- 3) охрана объектов и (или) имущества** на объектах с осуществлением работ по проектированию, монтажу и эксплуатационному обслуживанию технических средств охраны, перечень видов которых устанавливается Правительством РФ, и (или) с принятием соответствующих мер реагирования на их сигнальную информацию;
- 4) консультирование и подготовка рекомендаций клиентам** по вопросам правомерной защиты от противоправных посягательств;

- 5) обеспечение порядка в местах проведения массовых мероприятий;**
- 6) обеспечение внутриобъектового и пропускного режимов** на объектах, за исключением объектов, предусмотренных пунктом 7 настоящей части;
- 7) охрана объектов и (или) имущества, а также обеспечение внутриобъектового и пропускного режимов** на объектах, в отношении которых установлены обязательные для выполнения требования к антитеррористической защищенности, за исключением объектов, предусмотренных частью третьей статьи 11 настоящего Закона.

Организации, осуществляющие частную охранную деятельность, оказывают содействие правоохранительным органам в обеспечении правопорядка, в том числе в местах оказания охранных услуг и на прилегающих к ним территориях, а частные детективы оказывают содействие правоохранительным органам в предупреждении и раскрытии преступлений, предупреждении и пресечении административных правонарушений в порядке, установленном Правительством РФ.

## **Действия частных детективов (ст. 5)**

В ходе частной сыскной деятельности допускаются 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, наблюдение для получения необходимой информации в целях оказания услуг, перечисленных в части первой статьи 3 настоящего Закона.

При осуществлении частной сыскной деятельности допускается использование видео- и аудиозаписи, кино- и фотосъемки, технических и иных средств, не причиняющих вреда жизни и здоровью граждан и окружающей среде, в соответствии с законодательством РФ.

В ходе осуществления своей деятельности частный детектив обязан соблюдать законодательство РФ в части защиты информации, затрагивающей личную жизнь и имущество граждан.

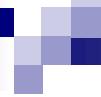
## **Частным детективам запрещается (ст. 7):**

- 1) скрывать от правоохранительных органов** ставшие им известными факты готовящихся, совершаемых или совершенных преступлений;
- 2) выдавать себя за сотрудников правоохранительных органов;**
- 3) собирать сведения, связанные с личной жизнью, с политическими и религиозными убеждениями отдельных лиц;**
- 4) осуществлять видео- и аудиозапись, фото- и киносъемку в служебных или иных помещениях без письменного согласия на то соответствующих должностных или частных лиц;**
- 5) прибегать к действиям, посягающим на права и свободы граждан;**
- 6) совершать действия, ставящие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан;**
- 7) фальсифицировать материалы или вводить в заблуждение клиента;**

- 8) разглашать собранные в ходе выполнения договорных обязательств сведения о заказчике, в том числе сведения, касающиеся вопросов обеспечения защиты жизни и здоровья граждан и (или) охраны имущества заказчика, использовать их в каких-либо целях вопреки интересам заказчика или в интересах третьих лиц, кроме как на основаниях, предусмотренных законодательством РФ;**
- 9) передавать свою лицензию для использования ее другими лицами;**
- 10) использовать документы и иные сведения, полученные в результате осуществления оперативно-розыскной деятельности органами, уполномоченными в данной сфере деятельности;**
- 11) получать и использовать информацию, содержащуюся в специальных и информационно-аналитических базах данных органов, осуществляющих оперативно-розыскную деятельность, в нарушение порядка, установленного законодательством РФ.**

## **Лицензия частным детективам не предоставляется (ст. 6):**

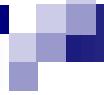
- 1) гражданам, не достигшим двадцати одного года;**
- 2) гражданам, состоящим на учете в органах здравоохранения по поводу психического заболевания, алкоголизма или наркомании;**
- 3) гражданам, имеющим судимость за совершение умышленного преступления;**
- 4) гражданам, которым предъявлено обвинение 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.**

**Удостоверение частного охранника** выдается сроком на пять лет. Срок действия удостоверения частного охранника может продлеваться в порядке, установленном Правительством РФ. Продление срока действия удостоверения частного охранника осуществляется только после прохождения профессионального обучения по программе повышения квалификации частных охранников в организациях, указанных в статье 15\_2 настоящего Закона (**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**).



**Руководитель частной охранной организации**  
должен иметь высшее образование и получить  
дополнительное профессиональное образование  
по программе повышения квалификации  
руководителей частных охранных организаций.  
Обязательным требованием является наличие у  
руководителя частной охранной организации  
удостоверения частного охранника. (ст. 15).

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

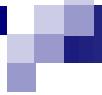
**- специальные средства,**

**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, предоставив при этом достаточно времени для выполнения своих требований, за исключением тех случаев, когда промедление в применении физической силы, специальных средств или огнестрельного оружия создает непосредственную опасность его жизни и здоровью или может повлечь за собой иные тяжкие последствия;
- стремиться в зависимости от характера и степени опасности правонарушения и лиц, его совершивших, а также силы оказываемого противодействия к тому, чтобы любой ущерб, причиненный при устраниении опасности, был минимальным;
- обеспечить лицам, получившим телесные повреждения, первую помощь и уведомить о произошедшем в возможно короткий срок органы здравоохранения и внутренних дел, территориальный орган федерального органа исполнительной власти, уполномоченного в сфере частной охранной деятельности;
- немедленно уведомить прокурора о всех случаях смерти или причинения телесных повреждений.



**Перечень видов специальных средств, используемых в частной охранной деятельности в соответствии с Постановлением Правительства «Вопросы частной детективной (сыскной) и частной охранной деятельности» от 14.08.1992 г. № 587:**

- 1) Шлем защитный 1-3 классов защиты отечественного производства;
- 2) Жилет защитный 1-5 классов защиты отечественного производства;
- 3) Наручники отечественного производства "БР-С", "БР-С2", "БКС-1", "БОС";
- 4) Палка резиновая отечественного производства "ПР-73М", "ПР-К", "ПР-Т", "ПУС-1", "ПУС-2", "ПУС-3".

**Виды вооружения охранников** (порядок приобретения, учета, хранения и ношения оружия регламентируются данным постановлением):

**1. Сертифицированные в установленном порядке в качестве служебного оружия:**

- а) огнестрельное гладкоствольное и нарезное короткоствольное оружие отечественного производства;
- б) огнестрельное гладкоствольное длинноствольное оружие отечественного производства;
- в) огнестрельное оружие ограниченного поражения отечественного производства.

**2. Сертифицированные в установленном порядке в качестве гражданского оружия:**

- а) огнестрельное оружие ограниченного поражения отечественного производства;
- б) газовые пистолеты и револьверы отечественного производства;
- в) механические распылители, аэрозольные и другие устройства, снаряженные слезоточивыми веществами, разрешенными к применению компетентным федеральным органом исполнительной власти;
- г) электрошоковые устройства и искровые разрядники отечественного производства, имеющие выходные параметры, соответствующие требованиям государственных стандартов РФ и нормам Минздрава России.

### **3. Сертифицированные в установленном порядке:**

- а) патроны к служебному оружию отечественного производства;
- б) патроны к гражданскому оружию травматического, газового и светозвукового действия, соответствующие нормам Минздрава России.

**Частные охранники обязаны проходить периодические проверки** на пригодность к действиям в условиях, связанных с применением огнестрельного оружия и (или) специальных средств. Содержание периодических проверок, порядок и сроки их проведения определяются федеральным органом исполнительной власти, уполномоченным в сфере частной охранной деятельности.

**Частные охранники** имеют право применять физическую силу в случаях, если настоящим Законом им разрешено применение специальных средств или огнестрельного оружия.

## **Охранники имеют право применять огнестрельное оружие в следующих случаях (ст. 18):**

- 1) для отражения нападения, когда его собственная жизнь подвергается непосредственной опасности;
- 2) для отражения группового или вооруженного нападения на охраняемое имущество;
- 3) для предупреждения (выстрелом в воздух) о намерении применить оружие, а также для подачи сигнала тревоги или вызова помощи;
- 4) для пресечения функционирования беспилотных аппаратов в целях, предусмотренных частью десятой статьи 12 настоящего Закона.

Запрещается применять огнестрельное оружие в отношении женщин, лиц с явными признаками инвалидности и несовершеннолетних, когда их возраст очевиден или известен охраннику, кроме случаев оказания ими вооруженного сопротивления, совершения вооруженного либо группового нападения, угрожающего жизни охранника или охраняемому имуществу, а также при значительном скоплении людей, когда от применения оружия могут пострадать посторонние лица.

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

**Федеральный государственный контроль** (надзор) за соблюдением законодательства РФ в области частной детективной деятельности и **федеральный государственный контроль** (надзор) за соблюдением законодательства РФ в области частной охранной деятельности осуществляют федеральный орган исполнительной власти, уполномоченный в сфере частной охранной деятельности, и его территориальные органы в пределах, установленных настоящим Законом, другими законами и иными нормативными правовыми актами РФ. Контроль за частной детективной деятельностью и частной охранной деятельностью на территории РФ осуществляют иные уполномоченные федеральные органы исполнительной власти и подчиненные им органы и подразделения в пределах, установленных настоящим Законом, другими законами и иными нормативными правовыми актами РФ.

**Надзор** за исполнением настоящего Закона осуществляют Генеральный прокурор Российской Федерации и подчиненные ему прокуроры.

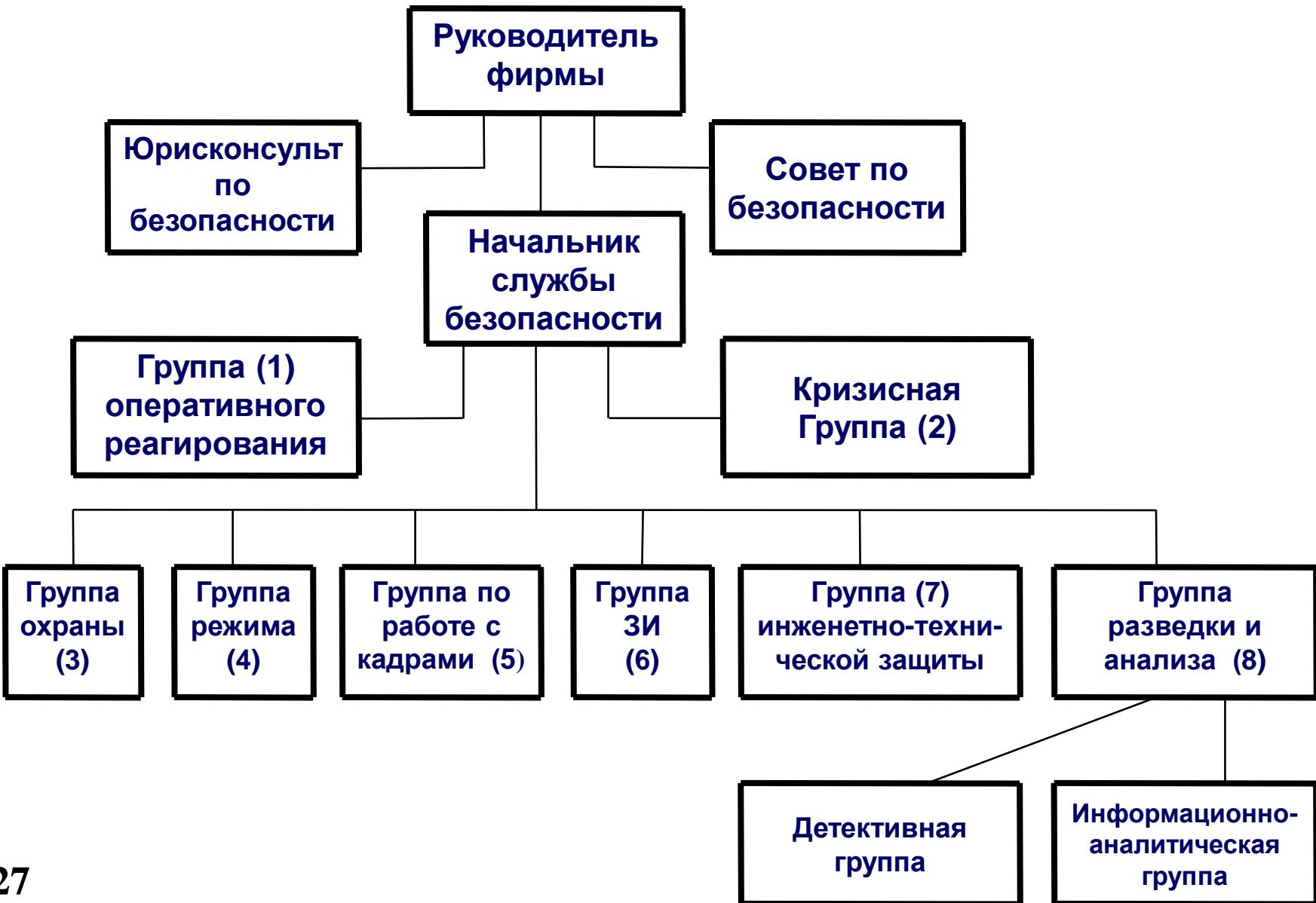
# **Задачи службы безопасности**

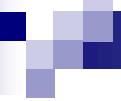
- 1. Определение сведений, составляющих КТ; лиц, имеющих к ним доступ; предприятий-партнеров на которых возможна утечка общих секретов.**
- 2. Выявление лиц и предприятий, проявляющих интерес к КТ предприятия.**
- 3. Разработка системы защиты документов с грифом КТ.**
- 4. Определение уязвимых участков 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 органами внутренних дел (ОВД).**

## **СБ для сохранения КТ принимает меры по**

- максимальному ограничению круга лиц, допускаемых к КТ;**
  - физической сохранности документов, содержащих такие сведения;**
  - обработке 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, главный 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:**

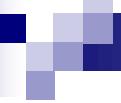
- при угрозе взрыва;**
- при захвате заложников или похищении сотрудников фирмы;**
- при вымогательстве;**
- при нападении на сотрудников и помещения фирмы;**
- при природных и техногенных катастрофах и т.п.**

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 01.07.1996 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, имеющим удостоверение частного охранника, действий, выходящих за пределы полномочий, установленных законодательством РФ, регламентирующим осуществление частной охранной и детективной деятельности, и повлекших существенное нарушение прав и законных интересов граждан и (или) организаций либо охраняемых законом интересов общества 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 принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, 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 **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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич**  
**Некрасов Алексей Валентинович**

## **Вопросы к подразделу 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 охранники 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 (ТЛФ) и линий связи (ЛС)

## Переизлучение самой конструкции аппарата.

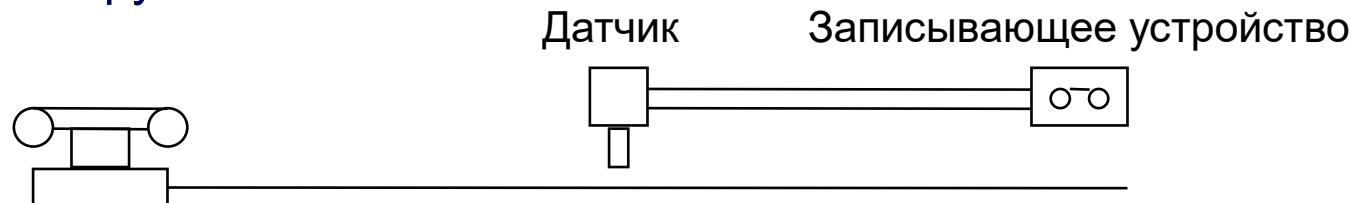
Старые кнопочные аппараты переизлучали информацию в радиусе до 200 м в диапазонах радиоволн СВ, КВ и УКВ. Средние волны (СВ) – длина волны 1000 – 100 м (частота 300 кГц – 3 МГц). Короткие волны (КВ) – длина волны 100 – 10 м (частота 3 – 30 МГц). Ультракороткие волны (УКВ) – длина волны 10 м – 0,1 мм (частота 30 МГц – 3000 ГГц).

**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 снятие модулированных речью колебаний (трубка не снята). Дальность съема информации этими способами – несколько десятков метров. Высокие частоты (ВЧ) – частота 3 – 30 МГц (длина волны 100 – 10 м).

**За счет наводки в проводе**, параллельном телефонному аппарату.

Датчик может быть на расстоянии до 20 см от самого провода. Способ трудно обнаружить.

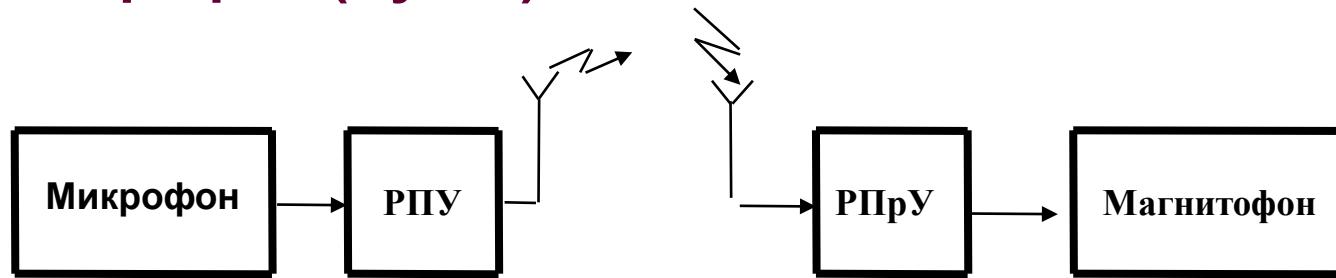


## 2. Вспомогательные технические средства и системы

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

## 3. Специальные технические средства сбора информации

### Радиомикрофон (жучок)

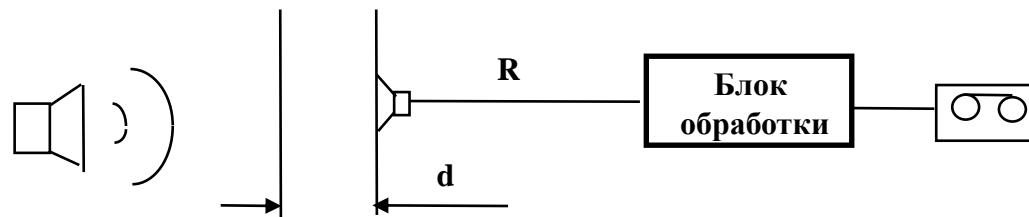


Структурная схема подслушивающего устройства

РПУ – радиопередающее устройство; РПрУ – радиоприемное устройство.

## Стетоскоп

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

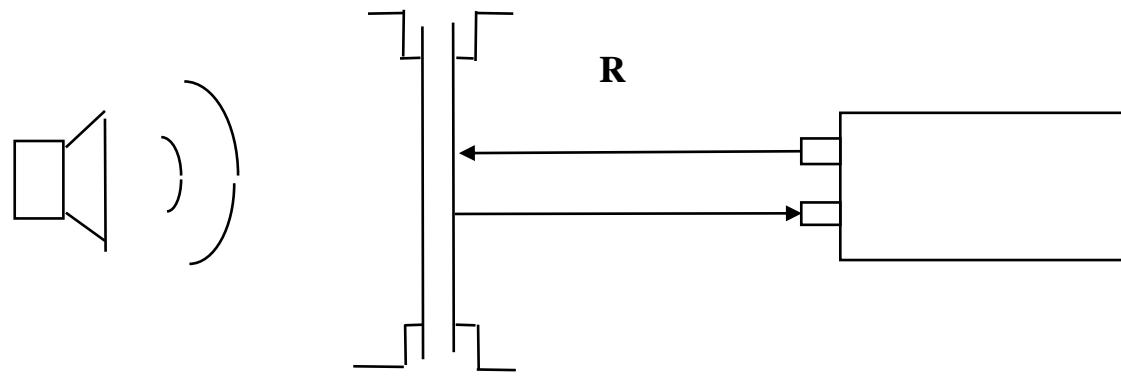


**Структурная схема использования стетоскопа**

При  $d$  до 1 м 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 электромагнитного (ЭМ) излучения элементов персонального компьютера (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 побочных  
электромагнитных излучений и наводок (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 другие нелинейные элементы.

## **2. Средства обеспечения скрытности информационного обмена**

**Скремблер** – шифровальное средство, предназначенное для защиты информации от непосредственного прослушивания за счет преобразования 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 сетчатке 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, дурнопахнущие;
- **вязкая пена**;
- **лазерные ослепители** (фонари).

## Детекторы лжи для мобильных телефонов

**Устройство** может подключаться к сотовому телефону и оценивать правдивость собеседника, 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 около 85%.

Для этого могут использоваться, например, технологии многослойного анализа голоса Sence и Layered Voice Analysis (LVA) израильской фирмы 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 других 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. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, - **наказываются штрафом до восьмидесяти тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.
2. То же деяние, совершенное лицом с использованием своего служебного положения, - **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 до четырехсот восьмидесяти часов, либо принудительными работами на срок до четырех лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок **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 четырех лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок **до четырех лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

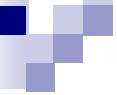
Примечание 1. Под специальными техническими средствами, предназначенными для негласного получения информации, в настоящем Кодексе понимаются приборы, системы, комплексы, устройства, специальные инструменты для проникновения в помещения и (или) на другие объекты и программное обеспечение для электронных вычислительных машин и других электронных устройств для доступа к информации и (или) получения информации с технических средств ее хранения, обработки и (или) передачи, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя.

Примечание 2. К специальным техническим средствам, предназначенным для негласного получения информации, не относятся находящиеся в свободном обороте приборы, системы, комплексы, устройства, инструменты бытового назначения, обладающие функциями аудиозаписи, видеозаписи, фотофиксации и (или) геолокации, с открыто расположеными на них органами управления таким функционалом или элементами индикации, отображающими режимы их использования, или наличием на них маркировочных обозначений, указывающих на их функциональное назначение, и программное обеспечение с элементами индикации, отображающими режимы его использования и указывающими на его функциональное назначение, если им преднамеренно путем специальной технической доработки, программирования или иным способом не приданы новые свойства, позволяющие с их помощью получать и (или) накапливать информацию, составляющую личную, семейную, коммерческую или иную охраняемую законом тайну, без ведома ее обладателя.

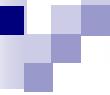
## **Регулирование деятельности, связанной со специальными техническими средствами**

**Указ Президента РФ «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» от 09.01.1996 г. № 21**  
**постановляет возложить на ФСБ:**

- лицензирование деятельности не уполномоченных на осуществление оперативно-розыскной деятельности физических и юридических лиц (далее именуются - неуполномоченные лица), связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввозом в Российскую Федерацию и вывозом за ее пределы специальных технических средств, предназначенных для негласного получения информации, а также, 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 12.04.2012 г. № 287  
введено “Положение о лицензировании деятельности по  
разработке, производству, реализации и приобретению в  
целях продажи специальных технических средств,  
предназначенных для негласного получения информации”**

Лицензиемую деятельность составляют следующие работы и услуги:

- а) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения и регистрации акустической информации;
- б) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного визуального наблюдения и документирования;
- в) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного прослушивания телефонных переговоров;
- г) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного перехвата и регистрации информации с технических каналов связи;

- д) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного контроля почтовых отправлений;
- е) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного исследования предметов и документов;
- ж) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного проникновения и обследования помещений, транспортных средств и других объектов;
- з) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного контроля за перемещением транспортных средств и других объектов;
- и) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи;
- к) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласной идентификации личности.

**Регламентируется также деятельность, связанная с применением радиоэлектронных средств (РЭС).**

**Постановлением Правительства РФ от 05.06.1994 г.  
№ 643 утверждено “Положение о порядке  
изготовления, ввоза в РФ и использования на  
территории РФ радиоэлектронных средств  
(высокочастотных устройств)”.**

**Под радиоэлектронным средством (высокочастотным устройством)** понимается техническое средство, состоящее из одного или нескольких радиопередающих или приемных устройств или их комбинации и вспомогательного оборудования.

**К радиоэлектронным средствам (высокочастотным устройствам)** относятся радиостанции, системы радионавигации, радиоопределения, системы кабельного телевидения и другие устройства, при работе которых используются радиочастоты выше 9 кГц.



## 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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**

## **Вопросы к подразделу 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).**

ГСЗИ представляет собой совокупность органов и исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации. Так же является составной частью системы обеспечения национальной безопасности РФ и призвана защищать безопасность государства от внешних и внутренних угроз в информационной сфере.

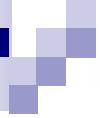
Организацию деятельности государственной системы защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной Государственной системой осуществляют ФСТЭК России.



**ГСЗИ** как система более сложная, включает в себя подсистемы лицензирования деятельности предприятий в области защиты информации, сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

**ГСЗИ 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 “Об организации лицензирования отдельных видов деятельности”** от 04.05.2011 № 99-ФЗ.

К ним, в частности, относятся (ст. 12):

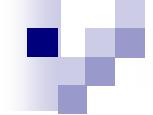
1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

- 2) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;
- 3) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- 4) разработка и производство средств защиты конфиденциальной информации;
- 5) деятельность по технической защите конфиденциальной информации.

Положениями о лицензировании конкретных видов деятельности устанавливаются исчерпывающие перечни выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности, в случае, если указанные перечни не установлены федеральными законами.

**Сертификация – это подтверждение соответствия**  
продукции или услуг установленным требованиям или  
стандартам.

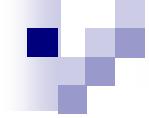
**Сертификат – документ, подтверждающий соответствие**  
средства ЗИ требованиям по безопасности информации.



## **Законодательной и нормативной базой лицензирования и сертификации в области ЗИ являются**

### **Законы РФ:**

- “О государственной тайне” от 21.07.1993 г. № 5485-1;
- “О техническом регулировании” от 27.12.2002 г. № 184-ФЗ;
- “О лицензировании отдельных видов деятельности” от 04.05.2011 г. № 99-ФЗ;
- “О защите прав потребителей” от 07.02.1992 г. № 2300-1.



## **Постановления Правительства РФ:**

- “Об организации лицензирования отдельных видов деятельности” от 21.11.2011 г. № 957;
- “О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны” от 15.04.1995 г. № 333;
- “О сертификации средств ЗИ” от 26.06.1995 г. № 608.
- “О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации” от 03.03.2012 г. № 171.
- “О лицензировании деятельности по технической защите конфиденциальной информации” от 03.02.2012 г. № 79.

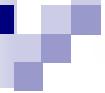
А также Указы Президента РФ, и ряд других подзаконных актов.

## **6.2. Лицензирование деятельности по защите ГТ**

**Общие нормы, устанавливающие порядок организации и осуществления этой деятельности, содержатся в ст. 27 "Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну" Закона "О государственной тайне".**

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путем получения ими в порядке, устанавливаемом Правительством РФ, лицензий на проведение работ со сведениями соответствующей степени секретности.

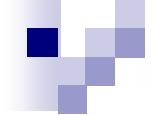
Лицензия на проведение указанных работ выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию.



Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий:

- выполнение требований нормативных документов, утверждаемых Правительством РФ, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;
- наличие в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;
- наличие у них сертифицированных средств защиты информации.

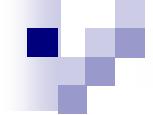
В периоды мобилизации, действия чрезвычайного или военного положения Президентом РФ может быть установлен иной порядок допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.



**Постановлением Правительства РФ № 333 от 15.04.1995 г.  
утверждено Положение о лицензировании деятельности  
предприятий, учреждений и организаций по проведению  
работ, связанных с использованием сведений,  
составляющих государственную тайну, созданием  
средств защиты информации, а также с осуществлением  
мероприятий и (или) оказанием услуг по защите  
государственной тайны.**

**В постановлении установлено, что:**

- лицензия разрешает осуществление конкретного вида  
деятельности в течение установленного срока на всей  
территории РФ, а также в учреждениях РФ,  
находящихся за границей;**
- органами, уполномоченными на ведение лицензионной  
деятельности, являются:**



**по допуску предприятий к проведению работ, связанных с использованием сведений, составляющих ГТ**

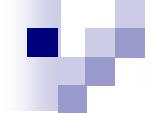
- ФСБ, СВР(за рубежом);

**на право проведения работ, связанных с созданием средств защиты информации**

- ФСТЭК, МО, 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 РФ, СВР и ФСТЭК по допуску к проведению работ, связанных с использованием сведений, составляющих ГТ, а также с осуществлением мероприятий и (или) оказанием услуг по защите ГТ, осуществляется руководителями министерств и ведомств РФ, которым подчинены указанные предприятия.**

Срок действия лицензии устанавливается в зависимости от специфики вида деятельности, но **не более чем на 5 лет**. По просьбе заявителя лицензия может выдаваться на срок менее 5 лет. Срок действия лицензии, выданной предприятию, не может превышать срока действия лицензии предприятия, структурное подразделение по защите ГТ которого оказывает услуги по защите ГТ.

Продление срока действия лицензии производится в порядке, установленном для ее получения.

Предприятие может иметь несколько лицензий.



## **Основанием для отказа в выдаче лицензии является:**

- наличие в документах, представленных заявителем, недостоверной или искаженной информации;**
- отрицательное заключение экспертизы, установившей несоответствие необходимым для осуществления заявленного вида деятельности условиям, указанным в пункте 7 настоящего Положения;**
- отрицательное заключение по результатам государственной аттестации руководителя предприятия.**

Специальная экспертиза предприятия проводится путем проверки выполнения требований нормативно-методических документов по режиму секретности, противодействию иностранным техническим разведкам и защите информации от утечки по техническим каналам, а также соблюдения других условий, необходимых для получения лицензии.

Специальные экспертизы проводятся на основе договора между предприятием и органом, проводящим специальную экспертизу. Расходы по проведению специальных экспертиз относятся на счет 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.



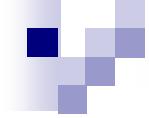
## Принципы лицензирования:

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 заявитель представляет в соответствующий орган, уполномоченный на ведение лицензионной деятельности, следующие документы:

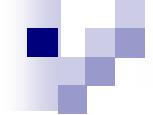
а) заявление о выдаче лицензии с указанием:

- наименования, организационно-правовой формы и местонахождения предприятия;
- идентификационного номера налогоплательщика;
- даты уплаты предприятием государственной пошлины за предоставление лицензии;
- сведений о наличии допуска к ГТ у руководителя предприятия;
- адресов мест осуществления лицензируемого вида деятельности;
- реквизитов правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;
- вида деятельности, на осуществление которого должна быть выдана лицензия;



- срока действия лицензии;
  - подтвержденной в установленном порядке степени секретности сведений, составляющих ГТ, с которыми заявитель предполагает проводить работы;
  - формы предоставления лицензии (на бумажном носителе или в электронной форме (в форме электронного документа, подписанного электронной подписью));
- б) копии учредительных документов юридического лица;
- в) копии правоустанавливающих документов на объекты недвижимости, необходимые для осуществления заявленного вида деятельности на срок действия лицензии, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним;
- г) копия договора об оказании услуг (в случае использования заявителем услуг структурного подразделения по защите ГТ другой организации).

**Проведение экспертизы осуществляется экспертными комиссиями Лицензионного центра либо Аттестационными центрами.**



Орган, уполномоченный на ведение лицензионной деятельности, принимает решение о выдаче или об отказе в выдаче лицензии в течение **30 дней** со дня получения заявления со всеми необходимыми документами.

В случае необходимости проведения дополнительной экспертизы предприятия решение принимается в **15-дневный срок** после получения заключения экспертизы, но не позднее чем через **60 дней** со дня подачи заявления о выдаче лицензии и необходимых для этого документов.

В зависимости от сложности и объема подлежащих специальной экспертизе материалов руководитель органа, уполномоченного на ведение лицензионной деятельности, может продлить срок принятия решения о выдаче или об отказе в выдаче лицензии до **30 дней**.

**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;**

Доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, хранение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

**- целостность;**

Целостность информации – термин в информатике (криптографии, теории телекоммуникаций, теории информационной безопасности), означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

**- конфиденциальность.**

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

# Государственная аттестация руководителей ответственных за защиту ГТ

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

Решением от 13.03.1996 г. № 3 Межведомственная комиссия по защите государственной тайны утвердила и ввела в действие "Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну".

**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;
- 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

Системы сертификации – это системы норм, правил, критериев качества продукции, методов их выявлений и оценки соответствия необходимым параметрам.

Системы сертификации могут быть международными, национальными и региональными. Национальный орган по сертификации определяется Правительством РФ.

В настоящее время национальным органом сертификации в РФ является **Росстандарт - Федеральное агентство по техническому регулированию и метрологии (ФАТРиМ)**.

На данный момент в России выделяется более 100 различных систем сертификации, которые в свою очередь подразделяются на обязательные и добровольные системы сертификации.

Обязательная система сертификации подразумевает, что проверка соответствия качества товара или услуги в этой системе установлена законодательно как обязательная, и реализация данного товара невозможна без оформления соответствующих документов в данной системе. Можно сказать, что самыми важными системами обязательной сертификации в России являются:

- Система сертификации ГОСТ Р;
- Система гигиенической (или санитарно-эпидемиологической) сертификации;
- Система пожарной сертификации.

Добровольные системы сертификации отличаются от обязательных только тем, что добровольный сертификат никто не может требовать. Однако, любая добровольная сертификация – это подтверждение качества товара или услуги, ответственности производителя.



Целями сертификации являются:

- **создание условий** для деятельности предприятий и предпринимателей на товарном рынке РФ и участия в международной торговле;
- **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.

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну также входит в перечень систем обязательной сертификации.

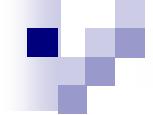
Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности (ст. 28. Порядок сертификации средств защиты информации Закона о государственной тайне).

**Организация сертификации средств ЗИ** возлагается на ФСТЭК, ФСБ и МО в соответствии с функциями, возложенными на них законодательством РФ.

Координация работ по организации сертификации средств ЗИ возлагается на межведомственную комиссию по защите ГТ.

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

**Положение о системе сертификации средств ЗИ**  
утверждено Приказом ФСТЭК России 03.04.2018 г. № 55  
и зарегистрировано в Министерстве юстиции РФ 11.05.2018 г.,  
регистрационный № 51063.



## **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.**

Сертификации в системе сертификации ФСТЭК России подлежат:

- средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;
- средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации;
- средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

Сертификация средств защиты информации иностранного производства, в отношении которых нормативными правовыми актами Российской Федерации установлены ограничения или запреты на их использование в Российской Федерации, в системе сертификации ФСТЭК России не осуществляется.

Сертификация средств защиты информации осуществляется на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России, а также техническими условиями, техническим заданием, заданием по безопасности, согласованными заявителями на сертификацию с ФСТЭК России (т.е. требованиями по безопасности информации).

## Система сертификации ФСТЭК России

Участниками системы сертификации ФСТЭК России являются:

- федеральный орган по сертификации;
- организации, аккредитованные ФСТЭК России в качестве органа по сертификации (далее – органы по сертификации);
- организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории (далее – испытательные лаборатории);
- изготовители средств защиты информации.

ФСТЭК России в соответствии с подпунктами 13 и 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 г. № 1085, организует проведение сертификации средств защиты информации, разрабатывает и устанавливает в пределах своей компетенции требования по безопасности информации к средствам защиты информации, а также в соответствии с Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26.06.1995 г. № 608, выполняет функции федерального органа по сертификации.

Органы по сертификации осуществляют сертификацию средств защиты информации, оформляют сертификаты соответствия средств защиты информации требованиям по безопасности информации (сертификат соответствия).

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют технические заключения и протоколы. Испытательные лаборатории должны обеспечивать полноту сертификационных испытаний средств защиты информации и достоверность их результатов.

Изготовители разрабатывают и (или) производят средства защиты информации в соответствии с требованиями по безопасности информации.

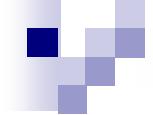
Изготовители средств защиты информации, составляющей государственную тайну, должны иметь лицензию ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну.

Изготовители средств защиты информации ограниченного доступа, не составляющей государственную тайну, должны иметь лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации.

Сертификация средств защиты информации осуществляется по следующим схемам:

- для единичного образца средства защиты информации – проведение испытаний образца средства защиты информации и проверки организации его технической поддержки;
- для партии средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его технической поддержки;
- для серийного производства средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его производства и технической поддержки.

Сертификация единичного образца или партии средства защиты информации организуется заявителем, планирующим применять средство защиты информации, в случае, если отсутствуют идентичные серийно производимые сертифицированные средства защиты информации. Сертификация серийного производства средства защиты информации организуется заявителем, осуществляющим разработку и (или) производство средства защиты информации.



Сертификационные испытания средств защиты информации проводятся на материально-технической базе испытательной лаборатории, а также на материально-технических базах заявителя и (или) изготовителя, расположенных на территории РФ.

Срок действия сертификата соответствия не может превышать **5 лет**. Сертификат соответствия выдается на срок, указанный в заявке на сертификацию.

Серийно производимое средство защиты информации считается сертифицированным, если оно произведено в период действия сертификата соответствия на его серийное производство, соответствует требованиям по безопасности информации и изготовитель и (или) заявитель осуществляют его техническую поддержку.

Для единичного образца или партии средства защиты информации срок действия сертификата соответствия не устанавливается.



## Порядок проведения сертификации средства защиты информации

Сертификация средства защиты информации включает следующие процедуры:

- подача заявки на сертификацию;
- принятие решения о проведении сертификации средства защиты информации;
- сертификационные испытания средства защиты информации;
- оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия;
- выдача (или отказ в выдаче) сертификата соответствия;
- предоставление дубликата сертификата соответствия;
- маркирование средств защиты информации;
- внесение изменений в сертифицированное средство защиты информации;
- переоформление сертификата соответствия;
- продление срока действия сертификата соответствия;
- приостановление действия сертификата соответствия;
- прекращение действия сертификата соответствия.



## 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.

Помимо этого в области ИТ действуют системы добровольной сертификации. Например, Система сертификации банковских технологий МЕКАС (ССБТ МЕКАС); Система добровольной сертификации услуг связи, средств связи и систем менеджмента качества организаций связи "Связь-Качество"; Система добровольной сертификации "Связь-Эффективность". Преимуществами наличия такого добровольного сертификата является повышение в разы конкурентоспособности компании на рынке и предоставляет ряд определенных выгод для бизнеса:

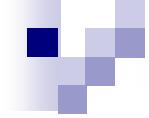
- повышение шансов на участие в конкурсных процедурах по выбору поставщика, проводимых в рамках государственных или коммерческих закупок;
- рост доверия заказчиков к предприятию;
- стимулирование спроса на услуги и расширение клиентской базы;
- формирование положительного имиджа фирмы;
- укрепление деловой репутации;
- рост эффективности маркетинговых кампаний;
- улучшение узнаваемости бренда;
- повышение инвестиционной привлекательности и капитализации бизнеса;
- выход на новые рынки и пр.

## **6.4. Аттестация объектов информатизации по требованиям безопасности информации**

Аттестация объектов информатизации по требованиям безопасности информации осуществляется системой аттестации объектов информатизации по требованиям безопасности информации, являющейся составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации, созданной Гостехкомиссией России и возглавляемой ею до 2005 г. С 2005 г. эту систему возглавляет ФСТЭК России.

Деятельность по аттестации объектов информатизации в названной системе осуществляется в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации», утвержденным председателем Государственной технической комиссии при Президенте РФ 25.11.1994 г.

Оно устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.



Под **аттестацией объектов информатизации** понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

В соответствии с п. 1.5 названного Положения обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей ГТ, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Расходы по проведению всех видов работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители.

## Организационная структура системы аттестации объектов информатизации:

- федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации – ФСТЭК России;
- органы по аттестации объектов информатизации по требованиям безопасности информации;
- испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

Порядок проведения аттестации объектов информатизации и осуществления государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации определяет раздел 3 названного Положения.

Проведение аттестации объектов информатизации по требованиям безопасности информации в соответствии с п. 3.1 раздела 3 названного Положения включает в себя следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- разработку программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрацию и выдачу "Аттестата соответствия";
- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
- рассмотрение апелляций.

Заключение по результатам аттестации с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи «Аттестата соответствия» и необходимыми рекомендациями подписывается членами аттестационной комиссии и доводится до сведения заявителя. К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод. Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Если объект информатизации отвечает (соответствует) требованиям по безопасности информации, органом по аттестации выдается «Аттестат соответствия» на этот объект заявителю.

«Аттестат соответствия» выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на **3 года**.

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации. В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

## **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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич**  
**Некрасов Алексей Валентинович**

## **Вопросы к подразделам 6.1, 6.2, 6.3 и 6.4**

- 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?**

## **6.5. 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 04.05.2011 г. № 99-ФЗ.**

**Положения настоящего ФЗ не применяются к отношениям, связанным с осуществлением лицензирования деятельности, связанной с защитой государственной тайны (ст. 2).**

Положениями о лицензировании конкретных видов деятельности устанавливаются исчерпывающие перечни выполняемых работ, оказываемых услуг, составляющих лицензируемый вид деятельности, в случае, если указанные перечни не установлены федеральными законами.

Лицензирование – деятельность лицензирующих органов по предоставлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, оценке соблюдения соискателем лицензии, лицензиатом лицензионных требований, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования.

Лицензия – специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается записью в реестре лицензий.

Лицензируемый вид деятельности – вид деятельности, на осуществление которого на территории РФ и на иных территориях, над которыми РФ осуществляет юрисдикцию в соответствии с законодательством РФ и нормами международного права, требуется получение лицензии в соответствии с настоящим Федеральным законом, в соответствии с федеральными законами, указанными в части 3 статьи 1 настоящего Федерального закона и регулирующими отношения в соответствующих сферах деятельности.

Лицензирующие органы – уполномоченные федеральные органы исполнительной власти и (или) их территориальные органы, органы исполнительной власти субъектов РФ, осуществляющие лицензирования в рамках полномочий субъектов РФ по предметам совместного ведения РФ и субъектов РФ, либо в случае передачи осуществления полномочий РФ в области лицензирования органам государственной власти субъектов РФ, а также Государственная корпорация по космической деятельности "Роскосмос".

Соискатель лицензии – юридическое лицо (в том числе иностранное юридическое лицо, если возможность осуществления лицензируемого вида деятельности иностранным юридическим лицом установлена в соответствии с частью 4 статьи 12 настоящего Федерального закона) или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии.

Лицензиат – юридическое лицо (в том числе иностранное юридическое лицо, если возможность осуществления лицензируемого вида деятельности иностранным юридическим лицом установлена в соответствии с частью 4 статьи 12 настоящего Федерального закона) или индивидуальный предприниматель, имеющие лицензию.

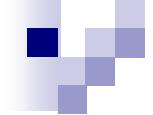
Лицензионные требования – обязательные требования, которые связаны с осуществлением лицензируемых видов деятельности, установлены положениями о лицензировании конкретных видов деятельности, основаны на соответствующих требованиях законодательства РФ и (или) положениях международных договоров РФ, не требующих издания внутригосударственных актов для их применения и действующих в РФ, направлены на обеспечение достижения целей лицензирования и оценка соблюдения которых осуществляется в порядке, предусмотренном настоящим Федеральным законом.

Место осуществления отдельного вида деятельности, подлежащего лицензированию (место осуществления лицензируемого вида деятельности) – производственный объект (здание, помещение, сооружение, линейный объект, территория, в том числе водные, земельные и лесные участки, транспортное средство и другой объект), который предназначен для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении, соответствует лицензионным требованиям, принадлежит соискателю лицензии или лицензиату на праве собственности либо ином законном основании, а также территория, которая предназначена для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении. Место осуществления лицензируемого вида деятельности имеет почтовый адрес и (или) другие данные, позволяющие его идентифицировать. Место осуществления лицензируемого вида деятельности может совпадать с местом нахождения соискателя лицензии или лицензиата. Положением о лицензировании конкретного вида деятельности может быть предусмотрено, что местом осуществления лицензируемого вида деятельности не могут являться помещения, здания, сооружения жилого назначения.

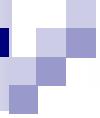
Уполномоченное должностное лицо лицензирующего органа – руководитель лицензирующего органа, иное должностное лицо лицензирующего органа, уполномоченное на принятие решения, осуществление иного действия в сфере лицензирования.

## **В соответствии с законом лицензированию подлежат следующие виды деятельности в области ЗИ (ст. 12):**

1) разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);



- 2) разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;
- 3) деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- 4) разработка и производство средств защиты конфиденциальной информации;
- 5) деятельность по технической защите конфиденциальной информации;
- 32) частная охранная деятельность;
- 33) частная детективная (сыскная) деятельность.



**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 ЭП.

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

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

Особенности лицензирования, в том числе в части, касающейся порядка принятия решения о предоставлении лицензии, срока действия лицензии и порядка продления срока ее действия, приостановления, возобновления и аннулирования действия лицензии, могут устанавливаться федеральными законами, регулирующими осуществление, например, следующих видов деятельности:

- оказание услуг связи, телевизионное вещание и (или) радиовещание;
- частная детективная (сыскная) деятельность и частная охранная деятельность.

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

Решение принимается в течении 45 рабочих дней.

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

1. Обеспечение соблюдения лицензиатом лицензионных требований осуществляется посредством проведения профилактических мероприятий, плановых контрольных (надзорных) мероприятий, внеплановых контрольных (надзорных) мероприятий в соответствии с Федеральным законом от 31.07.2020 г. N 248-ФЗ "О государственном контроле (надзоре) и муниципальном контроле в РФ", за исключением случаев, предусмотренных ч. 2 ст. 14.

Т.е. проводятся плановые проверки лицензиата.

Основания для их проведения:

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

А также проводятся и внеплановые проверки.

2. Проверка соблюдения лицензионных требований лицензиатами, осуществляющими лицензируемые виды деятельности, предусмотренные п. 1-5 и 18 ч. 1 ст. 12 настоящего ФЗ, осуществляется в соответствии с ФЗ от 26.12.2008 г. № 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" и нормативными правовыми актами федерального органа исполнительной власти в области обеспечения безопасности (в отношении лицензируемых видов деятельности, предусмотренных п. 1-3 и п. 4 (в части компетенции федерального органа исполнительной власти в области обеспечения безопасности) ч. 1 ст. 12 настоящего ФЗ) или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации (в отношении лицензируемых видов деятельности, предусмотренных п. 4 (в части компетенции федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации) и п. 5 ч. 1 ст. 12 настоящего ФЗ). Проверка соблюдения лицензионных требований лицензиатами, осуществляющими лицензируемые виды деятельности, предусмотренные п. 32 и 33 ч. 1 ст. 12 настоящего ФЗ, осуществляется в соответствии с законодательством, регулирующим осуществление частной охранной и частной детективной (сыскной) деятельности.

**Постановление Правительства РФ от 03.02.2012 г. № 79**  
**утвердило "Положение о лицензировании деятельности по технической защите конфиденциальной информации.**

Положение определяет **порядок лицензирования** деятельности по технической защите конфиденциальной информации (не содержащей сведений, составляющие государственную тайну, но защищаемой в соответствии с законодательством РФ), осуществляемой юридическими лицами и индивидуальными предпринимателями.

Под технической защитой конфиденциальной информации (ТЗКИ) понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.

**Лицензирование работ по ТЗКИ** осуществляют **ФСТЭК**.

При осуществлении лицензируемого вида деятельности  
лицензированию подлежат:

- а) услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам:
  - в средствах и системах информатизации;
  - в технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается;
  - в помещениях со средствами (системами), подлежащими защите;
  - в помещениях, предназначенных для ведения конфиденциальных переговоров (защищаемые помещения);
- б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- в) услуги по мониторингу информационной безопасности средств и систем информатизации;

г) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по ЗИ:

- средств и систем информатизации;
- помещений со средствами (системами) информатизации, подлежащими защите;
- защищаемых помещений;

д) работы и услуги по проектированию в защищенном исполнении:

- средств и систем информатизации;
- помещений со средствами (системами) информатизации, подлежащими защите;
- защищаемых помещений;

е) услуги по установке, монтажу, наладке, испытаниям, ремонту СЗИ (технических СЗИ, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) СЗИ, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

## **Лицензионными требованиями, предъявляемыми к соискателю лицензии на осуществление лицензируемого вида деятельности (лицензия), являются:**

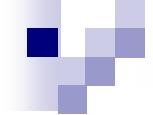
а) наличие у соискателя лицензии:

- юридического лица - в штате по основному месту работы в соответствии со штатным расписанием руководителя и (или) уполномоченного руководить работами по лицензируемому виду деятельности лица, имеющих высшее образование по направлению подготовки (специальности) в области ИБ и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, или высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, прошедших обучение по



программам профессиональной переподготовки по одной из специальностей в области ИБ (нормативный срок обучения - не менее 360 аудиторных часов), а также инженерно-технических работников (не менее 2 человек), имеющих высшее образование по направлению подготовки (специальности) в области ИБ и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области ИБ (нормативный срок обучения - не менее 360 аудиторных часов);

- индивидуального предпринимателя - высшего образования по направлению подготовки (специальности) в области ИБ и стажа работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, или высшего образования по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стажа работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, или иного высшего образования и стажа работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, а также дополнительного профессионального образования по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);



б) наличие по месту осуществления лицензируемого вида деятельности помещений, не являющихся объектами жилого назначения, принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, в которых созданы необходимые условия для размещения работников, производственного и испытательного оборудования для осуществления лицензируемого вида деятельности, обсуждения информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

- в) наличие принадлежащего соискателю лицензии на право собственности или ином законном основании, предусматривающем право владения и право пользования, оборудования, необходимого для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, в соответствии с определяемым Федеральной службой по техническому и экспортному контролю перечнем, в том числе:
- измерительных приборов, прошедших в установленном законодательством РФ порядке метрологическую поверку (калибровку);
  - программных (программно-технических) средств, включая средства контроля эффективности защиты информации, сертифицированных по требованиям безопасности информации, а также средств контроля (анализа) исходных текстов программного обеспечения;

- г) наличие по месту осуществления лицензируемого вида деятельности принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, автоматизированных систем, предназначенных для обработки конфиденциальной информации, средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством РФ;
- д) наличие технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, в соответствии с определяемым Федеральной службой по техническому и экспортному контролю перечнем. Документы, содержащие информацию ограниченного доступа, должны быть получены в установленном законодательством РФ порядке.

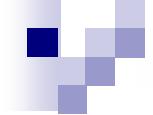
**Для получения лицензии соискатель лицензии  
направляет или представляет в лицензирующий орган  
следующие документы:**

- а) заявление о предоставлении лицензии с описью прилагаемых документов;
- б) копии документов, подтверждающих наличие в штате соискателя лицензии руководителя и (или) уполномоченного руководить работами по лицензируемому виду деятельности лица, инженерно-технических работников и их квалификацию (приказов о назначении или выписок из трудовых книжек, дипломов, удостоверений, свидетельств), и (или) сведения о трудовой деятельности, предусмотренные ст. 66\_1 ТК РФ;

- в) копии документов, подтверждающих наличие у соискателя лицензии по месту осуществления лицензируемого вида деятельности помещений, не являющихся объектами жилого назначения, необходимых для осуществления лицензируемого вида деятельности и принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях (зданиях, сооружениях);
- г) копии технических паспортов и аттестатов соответствия защищаемых помещений, находящихся по месту осуществления лицензируемого вида деятельности, требованиям безопасности информации;

- д) документы на автоматизированные системы, находящиеся в защищаемых помещениях по месту осуществления лицензируемого вида деятельности, предназначенные для обработки конфиденциальной информации, и средства защиты такой информации:
- копии технических паспортов автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации (с приложениями), актов классификации автоматизированных систем по требованиям безопасности информации, планов размещения основных и вспомогательных технических средств и систем, аттестатов соответствия автоматизированных систем требованиям безопасности информации или сертификатов соответствия автоматизированных систем требованиям безопасности информации;
  - перечень защищаемых в автоматизированных системах ресурсов;
  - описание технологического процесса обработки информации в автоматизированных системах;

- е) копии документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;
- ж) документы, содержащие сведения о наличии контрольно-измерительного, производственного и испытательного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и маркировании контрольно-измерительного оборудования, а также документов, подтверждающих права соискателя лицензии на использование указанного оборудования, средств защиты информации и средств контроля защищенности информации;



- з) документы, содержащие сведения об имеющихся технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 4 настоящего Положения, с приложением копий документов, подтверждающих, что документы, содержащие информацию ограниченного доступа, получены в установленном законодательством РФ порядке;
- и) копии документов, подтверждающих наличие необходимой системы производственного контроля в соответствии с установленными стандартами (при выполнении работ, указанных в подпункте "в" пункта 4 настоящего Положения).

**Постановление Правительства от 03.03.2012 г. № 171 утвердило  
Постановление "О лицензировании деятельности по  
разработке и производству средств защиты  
конфиденциальной информации".**

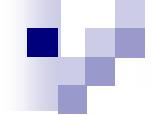
**Положение определяет порядок лицензирования деятельности  
по разработке и производству средств защиты  
конфиденциальной информации (не содержащей сведений,  
составляющие государственную тайну, но защищаемой в  
соответствии с законодательством РФ), осуществляемой  
юридическими лицами и индивидуальными  
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.**

При осуществлении деятельности по разработке и производству  
средств защиты конфиденциальной информации  
лицензированию подлежат следующие виды работ и услуг:

а) разработка средств защиты конфиденциальной информации, в  
том числе:

- 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;



б) производство средств защиты конфиденциальной информации, в том числе:

- 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;

**Если в качестве лицензирующего органа выступает ФСТЭК, лицензионными требованиями, предъявляемыми к соискателю лицензии на осуществление лицензируемого вида деятельности (далее - лицензия), являются:**

- а) наличие в штате у соискателя лицензии по основному месту работы в соответствии со штатным расписанием следующего квалифицированного персонала:**
- руководитель и (или) уполномоченное руководить работами по лицензируемому виду деятельности лицо, имеющие высшее образование по направлению подготовки (специальности) в области ИБ и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, или высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 7 лет, или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет, прошедшие обучение по программам профессиональной переподготовки по одной из специальностей в области ИБ (нормативный срок обучения - не менее 360 аудиторных часов);**

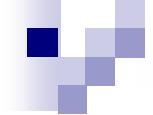
- инженерно-технические работники (не менее 2 человек), имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет или иное высшее образование и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет, прошедшие обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов);
- б) наличие по месту осуществления лицензируемого вида деятельности помещений, не являющихся объектами жилого назначения, принадлежащих соискателю лицензии на праве собственности или ином законном основании, предусматривающем право владения и право пользования, в которых созданы необходимые условия для размещения работников, производственного и испытательного оборудования, необходимого для осуществления лицензируемого вида деятельности, обсуждения информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

в) наличие принадлежащего соискателю лицензии на право собственности или ином законном основании, предусматривающем право владения и право пользования, оборудования, необходимого для выполнения работ и (или) оказания услуг, предусмотренных пунктом 3 настоящего Положения, в соответствии с определяемым Федеральной службой по техническому и экспортному контролю перечнем, в том числе:

- производственного и испытательного оборудования;
- измерительных приборов, прошедших в установленном законодательством РФ порядке метрологическую поверку (калибровку);
- программных (программно-технических) средств, включая средства контроля эффективности защиты информации, сертифицированных по требованиям безопасности информации, а также средств контроля (анализа) исходных текстов программного обеспечения;

г) наличие технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, предусмотренных пунктом 3 настоящего Положения, в соответствии с определяемым ФСТЭК перечнем.

Документы, содержащие информацию ограниченного доступа, должны быть получены в установленном законодательством РФ порядке;

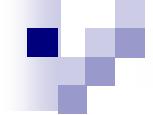


- д) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию (при выполнении работ, предусмотренных подпунктом "а" п. 3 настоящего Положения);
- е) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы производства средств защиты конфиденциальной информации, оценки качества выпускаемой продукции и неизменности установленных параметров, учета изменений, вносимых в техническую и конструкторскую документацию на производимую продукцию, учета готовой продукции (при выполнении работ, предусмотренных подпунктом "б" п. 3 настоящего Положения).

**Если в качестве лицензирующего органа выступает ФСБ России, лицензионными требованиями, предъявляемыми к соискателю лицензии, являются:**

- а) наличие в штате у соискателя лицензии на основной работе согласно штатному расписанию следующего квалифицированного персонала:
  - руководитель и (или) уполномоченное руководить работами по лицензируемому виду деятельности лицо, имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области проводимых работ по лицензируемому виду деятельности не менее 5 лет;
  - инженерно-технические работники (не менее 2 человек), имеющие высшее профессиональное образование по направлению подготовки "Информационная безопасность" в соответствии с Общероссийским классификатором специальностей и (или) прошедшие переподготовку по этой специальности (нормативный срок - свыше 100 аудиторных часов);

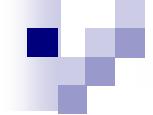
- б) наличие помещений для осуществления лицензируемого вида деятельности, соответствующих требованиям технической и технологической документации, национальных стандартов и методических документов в области защиты информации и принадлежащих соискателю лицензии на праве собственности или на ином законном основании, предусматривающем право владения и право пользования;
- в) наличие у соискателя лицензии на праве собственности или на ином законном основании, предусматривающем право владения и право пользования, контрольно-измерительного оборудования (прошедшего в соответствии с законодательством РФ метрологическую поверку (калибровку) и маркирование), производственного, испытательного оборудования и иных объектов, необходимых для осуществления лицензируемого вида деятельности;
- г) наличие предназначенных для осуществления лицензируемого вида деятельности программ (в том числе программных средств разработки средств защиты конфиденциальной информации) для электронно-вычислительных машин и баз данных, принадлежащих соискателю лицензии на праве собственности или на ином законном основании, предусматривающем право владения и право пользования;



- д) наличие аттестованных по требованиям безопасности информации средств обработки информации, используемых для разработки и производства средств защиты конфиденциальной информации, в соответствии с требованиями по защите информации;
- е) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию (при выполнении работ, предусмотренных подпунктом "а" пункта 3 настоящего Положения);
- ж) наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы производства средств защиты конфиденциальной информации, оценки качества выпускаемой продукции и неизменности установленных параметров, учета изменений, вносимых в техническую и конструкторскую документацию на производимую продукцию, учета готовой продукции (при выполнении работ, предусмотренных подпунктом "б" п. 3 настоящего Положения).

**Для получения лицензии соискатель лицензии направляет или представляет в лицензирующий орган следующие документы:**

- а) заявление о предоставлении лицензии с описью прилагаемых документов;**
- б) копии документов, подтверждающих наличие в штате соискателя лицензии специалистов по защите информации и их квалификацию (приказов о назначении или выписок из трудовых книжек, дипломов, удостоверений, свидетельств) и (или) сведения о трудовой деятельности, предусмотренные ст. 66\_1 ТК РФ;**
- в) копии правоустанавливающих документов на помещения, предназначенные для осуществления лицензируемого вида деятельности, права на которые не зарегистрированы в Едином государственном реестре прав на недвижимое имущество и сделок с ним (в случае, если такие права зарегистрированы в указанном реестре, - сведения об этих помещениях);**
- г) копии аттестатов соответствия защищаемых помещений требованиям по безопасности информации и технических паспортов, используемых для осуществления лицензируемого вида деятельности;**



- д) копии аттестатов соответствия средств обработки информации требованиям по безопасности информации и технических паспортов, используемых для осуществления лицензируемого вида деятельности;
- е) копии документов, подтверждающих право соискателя лицензии на программы для электронно-вычислительных машин и базы данных, планируемые к использованию при осуществлении лицензируемого вида деятельности;
- ж) сведения о наличии производственного, испытательного и контрольно-измерительного оборудования, средств защиты информации, средств разработки и производства средств защиты конфиденциальной информации, необходимых для осуществления лицензируемого вида деятельности, с приложением копий документов о поверке (калибровке) и марировании контрольно-измерительного оборудования, а также документов, подтверждающих право соискателя лицензии на использование указанных оборудования и средств;

- з) сведения об имеющихся технической и технологической документации, национальных стандартах и методических документах, необходимых для выполнения работ и (или) оказания услуг, предусмотренных п. 3 настоящего Положения, с приложением копий документов, подтверждающих, что документы, содержащие информацию ограниченного доступа, получены в установленном законодательством Российской Федерации порядке (в случае, если в качестве лицензирующего органа выступает Федеральная служба по техническому и экспортному контролю);
- и) копии документов, подтверждающих наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы разработки средств защиты конфиденциальной информации, учета изменений, вносимых в проектную и конструкторскую документацию на разрабатываемую продукцию (при выполнении работ, предусмотренных подпунктом "а" п. 3 настоящего Положения);

к) копии документов, подтверждающих наличие системы производственного контроля, включающей правила и процедуры проверки и оценки системы производства средств защиты конфиденциальной информации, оценки качества выпускаемой продукции и неизменности установленных параметров, учета изменений, вносимых в техническую и конструкторскую документацию на производимую продукцию, учета готовой продукции (при выполнении работ, предусмотренных подпунктом "б" п. 3 настоящего Положения).

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.

## **Схема последовательности действий при лицензировании**

- 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 информации (СЗИ) – это процесс, направленный на подтверждение соответствия СЗИ нормам и требованиям, действующим на территории России.

**Сертификация средств защиты кофиденциальной информации проводится в соответствии с Положением "О сертификации средств защиты информации", утвержденным ПП РФ от 26.06.1995 г. № 608.**

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, изложенными в нормативных документах ФСТЭК, в частности, в "Положении о системе сертификации средств защиты информации" утвержденном приказом ФСТЭК России от 03.04.2018 г. № 55.

В Евро-Азиатской ассоциации производителей товаров и услуг в области безопасности "ЕВРААС" действует **Система добровольной сертификации средств информационных технологий по требованиям информационной безопасности "АйТиСертифика"**. Система зарегистрирована в Росстандарте 30.06.2003 г. (регистрационный номер 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)**.



## 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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич**  
**Некрасов Алексей Валентинович**

## Вопросы к подразделу 6.5

- 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 представлены в Уголовном, Гражданском, Административном кодексах и других правовых актах.**

**Уголовное право регулирует отношения в области наиболее опасных правонарушений – преступлений.**

**Санкции за нарушение информационных правоотношений представлены в УК следующими статьями.**

## **Статья 128\_1. Клевета**

т.е. клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации либо совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть "Интернет", либо в отношении нескольких лиц, в том числе индивидуально не определенных.

## **Статья 137. Нарушение неприкосновенности частной жизни**

т.е. действия направленные на незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, включая те же деяния, совершенные лицом с использованием своего служебного положения.

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

**Статья 140. Отказ в предоставлении гражданину информации**

**Статья 141. Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий**

**Статья 142. Фальсификация избирательных документов, документов референдума, документов общероссийского голосования**

**Статья 144. Воспрепятствование законной профессиональной деятельности журналистов**

т.е. путем принуждения их к распространению либо к отказу от распространения информации.

## **Статья 146. Нарушение авторских и смежных прав**

## **Статья 147. Нарушение изобретательских и патентных прав**

## **Статья 180. Незаконное использование средств индивидуализации товаров (работ, услуг)**

т.е. незаконное использование чужого товарного знака, знака обслуживания, наименования места происхождения товара или сходных с ними обозначений для однородных товаров.

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

т.е. собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, обмана, шантажа, принуждения, подкупа или угроз, а равно иным незаконным способом, а также без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе.

**Статья 204. Коммерческий подкуп**

**Статья 205\_2. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма**

**Статья 207. Заведомо ложное сообщение об акте терроризма**

**Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей**

**Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов**

в т.ч. с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети "Интернет".

## **Статья 242\_1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних**

в т.ч. с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети "Интернет".

## **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 280. Публичные призывы к осуществлению экстремистской деятельности**

**Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства**

**Статья 283. Разглашение государственной тайны**

**Статья 283\_1. Незаконное получение сведений, составляющих государственную тайну**

**Статья 283\_2. Нарушение требований по защите государственной тайны**

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

**Статья 287. Отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации**

**Статья 298\_1. Клевета в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание, сотрудника органов принудительного исполнения Российской Федерации**

**Статья 354. Публичные призывы к развязыванию агрессивной войны**

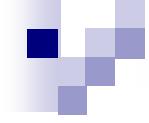
Перечисленные выше статьи УК РФ имеют важное значение в обеспечения законности и правопорядка в информационной сфере:

<https://krk.sledcom.ru/press/item/1331868/>

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

**Деятельность этих органов основывается на Законе РФ  
“Об оперативно-розыскной деятельности”, от 12.08.1995 г.  
№ 144-ФЗ.**

**Оперативно-розыскная деятельность (ОРД)** – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим ФЗ (далее – органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств (ст. 1).



## Задачи ОРД (ст. 2):

- выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших;
- осуществление розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, а также розыска без вести пропавших;
- добывание информации о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации;
- установление имущества, необходимого для обеспечения исполнения приговора в части гражданского иска, взыскания штрафа, других имущественных взысканий, или имущества, подлежащего конфискации.

**Принципы ОРД.** ОРД основывается на конституционных принципах законности, уважения и соблюдения прав и свобод человека и гражданина, а также на принципах конспирации, сочетания гласных и негласных методов и средств (ст. 3).

Сведения об используемых или использованных при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, и о лицах, оказывающих им содействие на конфиденциальной основе, а также об организации и о тактике проведения оперативно-розыскных мероприятий составляют государственную тайну и подлежат рассекречиванию только на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность (ст. 12, ст. 12\_1). В связи с этим в открытой литературе подобные сведения практически отсутствуют.

## **Оперативно-розыскными мероприятиями (ОРМ) предусматривается (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.
15. Получение компьютерной информации.



**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 с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, с получением компьютерной информации, проводятся с использованием оперативно-технических сил и средств органов ФСБ, ОВД в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность.

Ввоз в РФ и вывоз за ее пределы специальных технических средств (СТС), предназначенных для негласного получения информации, не уполномоченными на осуществление оперативно-розыскной деятельности физическими и юридическими лицами **подлежат лицензированию** в порядке, устанавливаемом Правительством РФ.

Перечень видов СТС, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, устанавливается Правительством РФ.

Разработка, производство, реализация и приобретение в целях продажи СТС, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность, **подлежат лицензированию** в соответствии с законодательством РФ (ст. 6).

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

Органам (должностным лицам), осуществляющим ОРД,  
запрещается:

- проводить оперативно-розыскные мероприятия в интересах какой-либо политической партии, общественного и религиозного объединения;
- принимать негласное участие в работе федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, а также в деятельности зарегистрированных в установленном порядке и незапрещенных политических партий, общественных и религиозных объединений в целях оказания влияния на характер их деятельности;
- разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и добре имя граждан и которые стали известными в процессе проведения оперативно-розыскных мероприятий, без согласия граждан, за исключением случаев, предусмотренных федеральными законами;



- подстрекать, склонять, побуждать в прямой или косвенной форме к совершению противоправных действий (provokacija);
- фальсифицировать результаты оперативно-разыскной деятельности (ст. 5).

В России применяется Система технических средств для обеспечения функций оперативно-разыскных мероприятий (СОРМ). СОРМ – это комплекс технических средств и мер, предназначенных для проведения оперативно-разыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи.

СОРМ обеспечивает два режима передачи информации:

- передача статистической информации;
- передача полной информации.

Различают 3 вида СОРМ:

СОРМ-1 – система прослушивания телефонных переговоров, организованная в 1996 г.;

СОРМ-2 – система протоколирования обращений к сети Интернет, организованная в 2000 г.

СОРМ-3 – обеспечивает сбор информации со всех видов связи и ее долговременное хранение. Она обеспечивает объединение всех вышеуказанных систем и дополнительно контролирует часть VPN серверов, прослушивает в прямом эфире Skype, ICQ, спутниковую связь и ряд других нововведений. Ключевой фактор СОРМ 3 – это единая глобальная база данных которая взаимно связана с различными направлениями СОРМ. Она сохраняет полную статистику о пользователе, анализируя все виды трафика: мобильный, интернет-трафик, переписку в мессенджерах и т.д. Система позволяет сохранять полный объем данных за конкретный период (до трех лет) или анализировать их в реальном времени.

**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:
  - признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела;
  - событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности РФ;
  - лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания;
  - лицах, без вести пропавших, и об обнаружении неопознанных трупов.

3. Поручения следователя, руководителя следственного органа, дознавателя, органа дознания или определения суда по уголовным делам и материалам проверки сообщений о преступлении, 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, осуществляемых уполномоченными на то государственными органами в порядке, предусмотренном законодательством РФ.
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 ОРД 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 предоставлении либо об аннулировании лицензии на осуществление частной детективной или охранной деятельности, о переоформлении документов, подтверждающих наличие лицензии, о выдаче (о продлении срока действия, об аннулировании) удостоверения частного охранника.

6\_1. О выдаче (предоставлении), переоформлении, об изъятии и (или) аннулировании лицензий на приобретение, экспонирование или коллекционирование оружия, разрешения на ношение и использование охотничьего оружия, разрешений на хранение, хранение и ношение, хранение и использование оружия и патронов к нему, их ввоз в Российскую Федерацию либо вывоз из Российской Федерации, а также о внесении изменений в реестры указанных лицензий и разрешений.

8. О достоверности сведений о законности происхождения денег, ценностей, иного имущества и доходов от них у близких родственников, родственников и близких лиц лица, совершившего террористический акт, при наличии достаточных оснований полагать, что деньги, ценности и иное имущество получены в результате террористической деятельности, но не ранее установленного факта начала участия лица, совершившего террористический акт, в террористической деятельности и (или) являются доходом от такого имущества.



**Проведение ОРМ (включая получение компьютерной информации), 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, совершаемого 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 или особо тяжкого преступления, а также при наличии данных о событиях и действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности РФ, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение ОРМ, предусмотренных частью второй настоящей статьи, 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 возникновения 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 (судьи) 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 6 месяцев.

## **Право осуществлять ОРД (ст. 13) на территории РФ предоставляется оперативным подразделениям:**

- 1. Органов внутренних дел РФ.**
- 2. Органов ФСБ.**
- 4. Федерального органа исполнительной власти в  
области государственной охраны.**
- 6. Таможенных органов РФ.**
- 7. Службы внешней разведки РФ.**
- 8. Федеральной службы исполнения наказаний.**

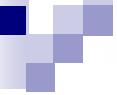
Оперативное подразделение органа внешней разведки Министерства обороны Российской Федерации проводит оперативно-розыскные мероприятия только в целях обеспечения безопасности указанного органа внешней разведки и в случае, если проведение этих мероприятий не затрагивает полномочий органов, указанных в пунктах 1, 2, 4, 6-8 части первой настоящей статьи.

## Контроль за ОРД

Контроль за ОРД осуществляют Президент, Федеральное Собрание РФ и Правительство РФ в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами. (ст. 20).

В соответствии со ст. 21 предусмотрен **прокурорский надзор** за ОРД. Прокурорский надзор за исполнением настоящего ФЗ закона осуществляют Генеральный прокурор РФ и уполномоченные им прокуроры.

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

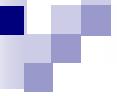


Отдельным законом регулируется деятельность ФСБ -  
**“О федеральной службе безопасности” от 03.04.1995 г.  
№ 40-ФЗ.**

ФСБ – единая централизованная система органов федеральной службы безопасности, осуществляющая решение в пределах своих полномочий задач по обеспечению безопасности РФ.

Правовую основу деятельности федеральной службы безопасности составляют Конституция РФ, настоящий ФЗ, другие федеральные законы и иные нормативные правовые акты РФ.

Деятельность ФСБ осуществляется также в соответствии с международными договорами РФ.



**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 консультации, 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, затрагивающие честь и достоинство гражданина или способные причинить вред его законным интересам, не могут сообщаться органами ФСБ кому бы то ни было без добровольного согласия гражданина, за исключением случаев, предусмотренных федеральными законами.

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



Должностные лица органов 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).

Наличие в информационных системах сведений о физических и юридических лицах не является основанием для принятия органами ФСБ мер, ограничивающих права указанных лиц.

Контроль за деятельностью органов ФСБ осуществляют Президент РФ, Федеральное Собрание РФ, Правительство РФ и судебные органы в пределах полномочий, определяемых Конституцией РФ, федеральными конституционными законами и федеральными законами (ст. 23).

Надзор за исполнением органами ФСБ законов РФ осуществляют Генеральный прокурор Российской Федерации и уполномоченные им прокуроры (ст. 24).

Сведения о лицах, оказывающих или оказывавших органам федеральной службы безопасности содействие на конфиденциальной основе, а также об организации, о тактике, методах и средствах осуществления деятельности органов федеральной службы безопасности в предмет прокурорского надзора не входят.

Имеются и другие правовые акты, регламентирующие деятельность этих органов. В ФЗ “О государственной гражданской службе РФ” от 27.07.2004 г. № 79-ФЗ указано, что государственный служащий обязан не разглашать сведения, составляющие государственную и иную охраняемую федеральным законом тайну, а также сведения, ставшие ему известными в связи с исполнением должностных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство (ст. 15).

## **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” от 26.07.2006 г. № 135-ФЗ.**
- 2. Закон РФ “О конкуренции и ограничении монополистической деятельности на товарных рынках”, от 22.03.1991 г. № 948-1.**
- 3. Закон РФ “О полиции” от 07.02.2011 г. № 3-ФЗ.**
- 4. Закона РФ “О санитарно-эпидемиологическом благополучии населения” от 30.03.1999 г. № 52-ФЗ.**
- 5. Закон РФ “О банках и банковской деятельности” от 01.12.1990 г. № 395-1 (в ред. ФЗ от 03.02.1996 г. № 17-ФЗ).**



Одной из форм недобросовестной конкуренции согласно закону “О защите конкуренции” является **недобросовестная конкуренция, связанная с незаконным получением, использованием или разглашением информации, составляющей коммерческую или иную охраняемую законом тайну (ст. 14\_7).**

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

В настоящее время функции федерального антимонопольного органа осуществляет Федеральная антимонопольная служба (ФАС) России. Положение о Федеральной антимонопольной службе утверждено Постановлением Правительства РФ от 29.07.2004 г. № 331.

ФАС является уполномоченным федеральным органом исполнительной власти, осуществляющим функции по принятию нормативных правовых актов и контролю за соблюдением антимонопольного законодательства, законодательства в сфере деятельности субъектов естественных монополий, в сфере государственного регулирования цен (тарифов) на товары (услуги), рекламы, контролю за осуществлением иностранных инвестиций в хозяйствственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства, контролю (надзору) в сфере государственного оборонного заказа, в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд и в сфере закупок товаров, работ, услуг отдельными видами юридических лиц, а также по согласованию применения закрытых способов определения поставщиков (подрядчиков, исполнителей) (ст. 1).



**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.**

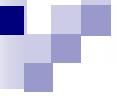
**В случае разглашения** сотрудниками ФАС сведений, составляющих КТ, причиненные убытки подлежат возмещению в соответствии с гражданским законодательством.

1. Информация, составляющая коммерческую, служебную, иную охраняемую законом тайну и полученная антимонопольным органом при осуществлении своих полномочий, не подлежит разглашению, за исключением случаев, установленных федеральными законами.
2. За разглашение информации, составляющей коммерческую, служебную, иную охраняемую законом тайну, работники антимонопольного органа несут гражданско-правовую, административную и уголовную ответственность.
3. 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 ФЗ “О защите конкуренции”).



Вопросы, связанные с полномочиями органов МВД  
отражены в ФЗ “О полиции” от 07.02.2011 г. № 3-ФЗ.

**Сотрудники полиции 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.**

## **Государственный контроль за деятельностью полиции**

осуществляют Президент РФ, палаты Федерального Собрания РФ, Правительство РФ в пределах полномочий, определяемых Конституцией РФ, федеральными конституционными законами и федеральными законами (ст. 49).

## **Прокурорский надзор за исполнением полицией**

**законов** осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры в соответствии с полномочиями, предоставленными федеральным законодательством (ст. 52).

## **Вред, причиненный гражданам и организациям**

противоправными действиями (бездействием) сотрудника полиции при выполнении им служебных обязанностей, подлежит возмещению в порядке, установленном законодательством РФ (ст. 33).

**Значительными полномочиями по проверке соблюдения на предприятиях санитарных правил, норм и гигиенических нормативов обладают должностные лица и специалисты Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор) (ранее эту роль выполняла Государственная санитарно-эпидемиологическая служба РФ).**

Роспотребнадзор является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере защиты прав потребителей, здорового питания, в области организации питания, обеспечения качества и безопасности пищевых продуктов, материалов и изделий, контактирующих с пищевыми продуктами, разработке и утверждению государственных санитарно-эпидемиологических правил и гигиенических нормативов, а также по организации и осуществлению федерального государственного санитарно-эпидемиологического контроля (надзора), федерального государственного контроля (надзора) в области защиты прав потребителей и федерального государственного контроля (надзора) за соблюдением законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или)

развитию, федерального государственного лицензионного контроля (надзора) за деятельностью в области использования возбудителей инфекционных заболеваний человека и животных (за исключением случая, если указанная деятельность осуществляется в медицинских целях) и генно-инженерно-модифицированных организмов III и IV степеней потенциальной опасности, осуществляющейся в замкнутых системах, федерального государственного лицензионного контроля (надзора) за деятельностью в области использования источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности) (ст. 1 «Положения о Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека», утвержденного постановлением Правительства РФ от 30.06.2004 г. № 322).

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.



Закон РФ “О банках и банковской деятельности” от 02.12.1990 г. № 396-1 **устанавливает, что кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов.**

(Банк-корреспондент – это банк, состоящий в деловых отношениях с другими банками и выполняющий платежи, расчеты, иные операции по их поручению и за их счет на основе корреспондентского договора. Для выполнения поручений банки-корреспонденты открывают специальные корреспондентские счета.)

**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 (ст. 26).**



**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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич**  
**Некрасов Алексей Валентинович**



## 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?**

## **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 Союзного государства (Республика Беларусь и РФ) таких тайн более 50.**

**В законе «Об информации, информационных технологиях и о защите информации» нет термина «конфиденциальная информация», но дается определение понятия «конфиденциальность информации».**

**Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.**



Указом Президента Российской Федерации "Об утверждении перечня сведений конфиденциального характера" от 06.03.1997 г. № 188 был утвержден «Перечень сведений конфиденциального характера», где указаны:

**Коммерческая тайна**

**Служебная тайна**

**Профессиональная тайна**

**Персональные данные**

**Тайна следствия и судопроизводства**

**Сведения о защищаемых лицах и мерах государственной защиты**

**Сведения о сущности неопубликованных изобретений**

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.

**В действующем законодательстве наименее разработанными являются профессиональная тайна и служебная тайна.**

## Грифы конфиденциальности

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

Так, в соответствии с международными стандартами в западных странах чаще используются следующая классификация:

- открытая информация (**ОИ**) – Public;
- для внутреннего использования (**ДВИ**) – Internal;
- конфиденциальная информация (**КИ**) – Confidential;
- строго конфиденциальная информация (**СКИ**) – Strictly Confidential.

На основе российского законодательства предпочтительнее применять следующее разграничение информации по грифу конфиденциальности:

- открытая информация (**ОИ**);
- для внутреннего использования (**ДВИ**);
- конфиденциальная информация (**КИ**).

## **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 определением профессиональной тайны 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, включающие в себя и профессиональную тайну:**

### **1. Законы РФ :**

**ГК РФ** (ст. 152.2. Охрана частной жизни гражданина);

**УК РФ** (ст. 155. Разглашение тайны усыновления (удочерения));

**ГПК РФ** (ст. 10. Гласность судебного разбирательства);

**УПК РФ** (ст. 53. Полномочия защитника);

**Семейный кодекс РФ** (ст. 15. Медицинское обследование лиц, вступающих в брак, ст. 139. Тайна усыновления ребенка);

**ФЗ «О связи»** (ст. 63. Тайна связи) от 07.07.2003 г. № 126-ФЗ;

**ФЗ «Об основах охраны здоровья граждан в РФ»** от 21.11.2011 г. № 323-ФЗ (ст. 13. Соблюдение врачебной тайны, ст. 73. Обязанности медицинских работников и фармацевтических работников);

**Закон «О психиатрической помощи и гарантиях прав граждан при ее оказании»** от 02.07.1992 г. (ст. 9. Сохранение врачебной тайны при оказании психиатрической помощи, ст. 46. Контроль общественных объединений за соблюдением прав и законных интересов граждан при оказании психиатрической помощи);

**ФЗ «О свободе совести и о религиозных объединениях» от 26.09.1997 г. № 125-ФЗ** (ст. 3. Право на свободу совести и свободу вероисповедания);

**ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»** от 31.05.2002 г. № 63-ФЗ (ст. 8. Адвокатская тайна);

**Закон «Основы законодательства РФ о нотариате»** от 10.02.1993 г. № 4462-1 (ст. 5. Гарантии нотариальной деятельности, ст. 14. Присяга нотариуса, ст. 16. Обязанности нотариуса, ст. 17. Ответственность нотариуса, ст. 28. Обязанность нотариусов представлять сведения нотариальной палате, ст. 34. Контроль за исполнением нотариусами профессиональных обязанностей);

**Закон «О трансплантации органов и (или) тканей человека»** от 22.12.1992 г. № 4180-1 (ст. 14. Ответственность за разглашение сведений о доноре и реципиенте);

**ФЗ «Об основах социального обслуживания граждан в РФ»** от 28.12.2015 г. № 122-ФЗ (ст. 6. Конфиденциальность информации о получателе социальных услуг);

**ФЗ «О средствах массовой информации»** от 27.12.1991 г. № 2124-1 (ст. 41. Обеспечение конфиденциальности информации).

## **2. Подзаконные акты**

### **Постановления Правительства РФ:**

«О заключении межправительственных соглашений об избежании двойного налогообложения доходов и имущества» от 24.02.2010 г.

№ 84 (ст. 26. Обмен информацией);

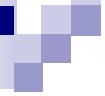
«Правила оказания услуг телефонной связи» (п. 4. Оператор связи обязан обеспечить соблюдение тайны телефонных переговоров, передаваемых по сетям связи.) утверждены ПП РФ «О порядке оказания услуг телефонной связи» от 09.12.1997 г. № 1342;

«Правила проведения обязательного медицинского освидетельствования на выявление вируса иммунодефицита человека (ВИЧ-инфекции)» утверждены ПП РФ «Об утверждении правил обязательного медицинского освидетельствования на выявление ВИЧ-инфекции» от 20.10.2020 г. № 1129н (п. 8.

Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском освидетельствовании на выявление ВИЧ-инфекции, составляют врачебную тайну);

«Правила оказания услуг почтовой связи» утверждены ПП РФ от 17.04.2023 г. № 382 «Об утверждении правил оказания услуг почтовой связи:

- п. 46. Операторы почтовой связи обязаны: г) соблюдать тайну связи,
  - п. 47. Информация об адресных данных пользователей услугами почтовой связи, о почтовых отправлениях, почтовых переводах, телеграфных и иных сообщениях, входящих в сферу деятельности операторов почтовой связи, а также сами эти почтовые отправления, переводимые денежные средства, телеграфные и иные сообщения являются тайной связи и выдаются только отправителям (адресатам) или их уполномоченным представителям,
  - п. 48. Обработка персональных данных пользователей услугами почтовой связи в соответствии с пунктами 30 и 33 настоящих Правил осуществляется с соблюдением требований, установленных законодательством Российской Федерации в области персональных данных.
- и другие подзаконные акты.



### **3. Судебная практика:**

**Постановление Конституционного суда РФ от 27.03.1996**

г. № 8-П (в части профессиональной тайны адвоката)

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_9861/](https://www.consultant.ru/document/cons_doc_LAW_9861/);

**Постановление Пленума Верховного суда РФ от**

**15.11.2022 г. № 33 «О практике применения судами норм  
о компенсации морального вреда»**

<http://www.supcourt.ru/documents/own/31761/>

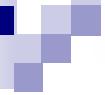
и др.

### **4. Международные договоры и соглашения**

Более 80 двусторонних соглашений об избежании двойного  
налогообложения доходов и имущества

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_214195/](https://www.consultant.ru/document/cons_doc_LAW_214195/)

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**

**Адвокатская тайна**

**Тайна исповеди**

**Тайна связи**

**Тайна усыновления**

**Журналистская тайна**

**Нотариальная тайна**

**Тайна страхования**

## **Законы РФ:**

**"Основы законодательства РФ о нотариате"**

**"О средствах массовой информации"**

**"Семейный кодекс РФ"**

- (Тайна усыновления - уголовная ответственность за разглашение)
- (Тайна связи - уголовная ответственность за разглашение).
- (Нет доступа со стороны государственных органов к адвокатской тайне).

**"Об адвокатской деятельности и адвокатуре РФ"**

- (Нет доступа со стороны государственных органов к тайне исповеди).

**"О свободе совести и о религиозных объединениях"**



## **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 до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.**



## **2. То же деяние, совершенное лицом с использованием своего служебного положения, -**

**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  
до четырехсот восьмидесяти часов, либо  
принудительными работами на срок до четырех лет, либо  
арестом на срок до четырех месяцев, либо лишением  
свободы на срок до четырех лет.**

## **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 обязательными работами на срок до трехсот шестидесяти часов, 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.

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 утечке этой информации страдают интересы службы (а не клиентов, как в случае профессиональной тайны).**

До 2008 года в Гражданском кодексе РФ существовало понятие служебной тайны. Статья 139 ГК РФ закрепила, что информация является служебной тайной, когда она имеет коммерческую ценность в силу ее неизвестности третьим лицам. С принятием Федерального закона от 18.12.2006 г. № 231-ФЗ указанная статья ГК утратила силу. На охрану коммерческой тайны встал закон «О коммерческой тайне», а вот понятие служебной тайны осталось в подзаконных актах. Ни федеральный закон, ни какой-либо кодекс не содержат прямого определения служебной тайны, но сам термин остается в действующем ТК, КоАП и других актах. Исходя из действующих нормативных актов, понятие служебной тайны можно определить следующим образом:

**Служебная тайна** – это защищаемая конфиденциальная информация, доступ к которой ограничен законом, ставшая известной сотрудникам организаций при исполнении ими служебных обязанностей.

**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).**

Служебная тайна не относится к коммерческой тайне. Служебная тайна – это служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (Указ Президента РФ от 06.03.1997 г. № 188). А коммерческая тайна – это информация, которая имеет действительную или потенциальную коммерческую ценность в силу того, что она неизвестна третьим лицам и охраняется обладателем.

То есть служебная тайна – это сведения конфиденциального характера о деятельности органов государственной, региональной или муниципальной власти. В это понятие также входят сведения ограниченного характера, в отношении которых предпринимаются действия по защите конфиденциальности и которые были получены законным путем в процессе исполнения должностных обязанностей госслужащими и сотрудниками перечисленных органов власти. Таким образом, отличительная особенность информации, относящейся к служебной тайне, заключается в том, что ее носителем является какой-либо государственный орган. То есть в коммерческой организации или у работодателя-физического лица не возникает необходимости охранять служебную тайну. Обязанность работника не разглашать коммерческую или служебную тайну может быть установлена в **трудовом договоре, должностной инструкции или в отдельном положении о служебной тайне**.

Понятие служебной и профессиональной тайны также отличаются.

Профессиональная тайна – это сведения, которые стали известны при выполнении профессиональной деятельности. В качестве примеров профессиональной тайны упоминается врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.п.

Служебная тайна регулируется актами специального назначения, которые направлены на деятельность работников государственного аппарата.

Профессиональная тайна, в свою очередь, направлена на широкий круг специалистов и регулируется отдельным профильными законами.

В состав профессиональной тайны входят перечень сведений, которые относятся к той или иной профессии. Например, тайна журналиста, тайна исповеди и пр. Состав же служебной тайны определяется внутренними регламентами работы государственных и муниципальных органов. Например, следователь в ходе расследования уголовного дела будет опираться на внутренний регламент для защиты служебной тайны следственного отдела.



Есть сведения, которые нельзя однозначно отнести к профессиональной или служебной тайне. Например, персональные данные гражданина могут составить служебную тайну для прокурора, который рассматривает дело и является госслужащим. А для работника кадровой службы эти персональные данные будут являться профессиональной тайной.

Перечень сведений, которые составляют служебную тайну, можно выделить из определения служебной тайны (Положение о порядке обращения со служебной информацией ограниченного распространения, утв.

Постановлением Правительства РФ от 03.11.1994 г. № 1233). Так, к служебной тайне относятся:

- сведения, которые касаются работы государственных органов или подведомственных организаций;
- сведения, которые получили работники этих учреждений в рамках исполнения своих должностных обязанностей о других лицах и структурах. (Это может быть личная, профессиональная, коммерческая информация, которая не подлежит разглашению.);
- тайна предварительного следствия и судебная тайна, включающая в себя тайну работы судей и присяжных;
- сведения, доступ к которым ограничил федеральный закон с целью защиты интересов государства.

Есть и другая классификация, которая поможет раскрыть сведения, которые относятся к служебной тайне. Так, к служебной тайне относятся:

- следственная;
- налоговая;
- судебная;
- военная тайна;
- конфиденциальная информация, которая составляет коммерческую, банковскую, профессиональную тайну или тайну личной жизни, которую служащий получил в ходе исполнения своих обязанностей.

Таким образом, условия отнесения информации к служебной тайне определяет закон. Можно выделить три критерия, по которым информация может быть отнесена к служебной тайне:

- она не составляет государственную тайну;
- она не является общедоступной;
- обеспечить ее сохранность и ограничить несанкционированный доступ можно в режиме профессиональной или служебной тайны.

Некоторые специалисты считают, что адвокатская и врачебная тайна относятся к служебной. Но врачи и адвокаты не являются государственными или муниципальными служащими и сведения, которые они получили в ходе работы, относятся к профессиональной тайне, а не к служебной.



Федеральный закон «Об информации, информационных технологиях и о защите информации» (от 27.07.2006 г. № 149-ФЗ), а также «Положение о порядке обращения со служебной информацией ограниченного распространения» содержит перечень сведений, которые не могут составлять служебную тайну:

1. Нормативно-правовые акты, которые затрагивают права, обязанности, свободы граждан.
2. Информация о состоянии окружающей среды (о чрезвычайных ситуациях, опасных природных явлениях), и необходимая для обеспечения безопасного существования населенных пунктов, производственных объектов, граждан и населения в целом.
3. Информация о деятельности государственных органов и органов местного самоуправления.
4. Порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц в органы государственной власти.
5. Сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения.
6. Информация в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах.

Служебная тайна относится к конфиденциальной информации. Поэтому закон предъявляет к ней особые меры защиты. Так, в целях защиты служебной информации необходимо принять меры, которые должны обеспечить:

- защиту от несанкционированного доступа, копирования, уничтожения, внесения изменений, блокирования и тиражирования сведений, составляющих служебную тайну;
- сохранение конфиденциальности;
- реализацию права на доступ только ограниченному кругу лиц, имеющих официальное разрешение.

Необходимые меры по защите служебной тайны – разработка локальных нормативных актов, напр., «Положение о порядке обращения со служебной информацией ограниченного пользования». Этим регламентом определяют категории должностей, которым в силу служебной необходимости будет открыт доступ к такого рода сведениям, а также порядок обращения с ними и передачи по запросам в другие органы государственной власти.

Положением необходимо установить порядок присвоения и снятия статуса «Для служебного пользования» документам в организации, а также меры, направленные на защиту такой информации и документов.

Положение о защите служебной тайны не относится к тем, что в соответствии с ТК должны согласовываться с представительным органом работников. Работодатель вправе разработать и утвердить его самостоятельно.

**Доступ к документам**, которые содержат служебную тайну, работникам

учреждения производится только под расписку. При необходимости передать сведения в другие органы или организации используется защищенный канал связи или пересылка заказными или ценными отправлениями. Копии со служебных документов разрешается делать только по распоряжению руководителя. Все бумаги, составляющие служебную тайну, должны храниться в запираемых хранилищах.

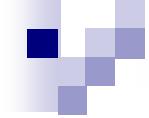
Работники, которые имеют доступ к служебной тайне, должны подписать отдельный договор или соглашение о **неразглашении служебной тайны**. Условие о запрете распространять эту тайну можно также закрепить в его трудовом договоре.

Если государственный или муниципальный служащий разгласит служебную тайну, его можно уволить по инициативе работодателя по п. 6 ст. 81 ТК. В этом случае работодатель должен зафиксировать нарушение, далее запросить у работника письменные объяснения по факту разглашения коммерческой тайны (ч. 1 ст. 193 ТК). Уволить работника можно будет не позднее месяца со дня обнаружения проступка (ч. 3 ст. 193 ТК).

Все документы, которые содержат конфиденциальные сведения, должны иметь соответствующую пометку: «для служебного пользования». Право присваивать определенным документам такой статус есть у должностных лиц, уполномоченных на это руководителем федерального органа исполнительной власти. Он же организует порядок:

- передачи сведений, составляющих служебную тайну, другим государственным органам или организациям;
- снятия отметки «для служебного пользования» с документов (информационных носителей и других источников);
- защиты служебной информации от распространения третьим лицам.

В свою очередь, сотрудники госорганов, которые имеют право присваивать сведениям и информации статус служебной тайны, несут ответственность за обоснованность своих действий. То есть для установления пометки «для служебного пользования» должны быть весомые основания. Кроме того, ответственный за защиту служебной тайны ведет обязательный учет документов и своевременно уничтожает документы с конфиденциальными сведениями.



За разглашение служебной тайны для должностных лиц предусмотрена различная ответственность. В первую очередь, Трудовым кодексом установлено право работодателя применить в случае разглашения работником охраняемой тайны дисциплинарное взыскание вплоть до увольнения (п. 6 ст. 81 ТК РФ). В этом случае в трудовой книжке указывается причина увольнения со ссылкой на статью ТК РФ.

В ст. 13.14 КоАП также предусмотрено наказание за разглашение информации с ограниченным доступом:

- для граждан штраф составляет от 500 руб. до 1000 руб.;
- для должностных лиц — от 4000 руб. до 5000 руб.

## **Законодательные документы в отношении защиты служебной тайны:**

1. ФЗ “О государственной гражданской службе РФ” от 27.07.2004 г. № 79-ФЗ.
2. ФЗ “О прокуратуре РФ” от 17.01.1992 г. № 2202-1.
3. ФЗ “О банках и банковской деятельности” от 02.12.1990 г. № 395-1.
4. ФЗ “О полиции” от 07.02.2011 г. № 3-ФЗ.
5. ФЗ “Об оперативно-розыскной деятельности” от 12.08.1995 г. № 144-ФЗ.
6. ФЗ “О связи” от 07.07.2003 г. № 126-ФЗ.
7. ФЗ РФ "О коммерческой тайне" от 29.07.2004 г. № 98-ФЗ.
8. Уголовный кодекс РФ от 13.06.1996 г. № 63-ФЗ.
9. Таможенный кодекс Евразийского экономического союза  
(приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза, ратифицирован ФЗ от 14.11.2017 г. № 317-ФЗ).
10. "Правила обращения со сведениями, составляющими служебную тайну в области обороны" утв. ПП РФ от 26.11.2021 г. № 2052.

## Налоговая тайна

**Понятие налоговой тайны (НТ) введено Налоговым кодексом РФ.** Согласно п. 1 ст. 102 налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, плательщике страховых взносов.

**Режим хранения сведений, составляющих НТ, и доступа к ним устанавливается Федеральной налоговой службой (ФНС России).**

Налоговая тайна не подлежит разглашению налоговыми органами, органами внутренних дел, следственными органами, органами государственных внебюджетных фондов и таможенными органами, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных федеральным законом (п. 2 ст. 102).

К разглашению налоговой тайны относится, в частности, использование или передача другому лицу информации, составляющей коммерческую тайну (секрет производства) налогоплательщика, плательщика страховых взносов и ставшей известной должностному лицу налогового органа, органа внутренних дел, следственного органа, органа государственного внебюджетного фонда или таможенного органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей (п. 2 ст. 102).

Поступившие в налоговые органы, органы внутренних дел, следственные органы, органы государственных внебюджетных фондов или таможенные органы сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа (п. 3 ст. 102).

Режим хранения сведений, составляющих НТ, и доступа к ним устанавливается Федеральной налоговой службой (ФНС России).

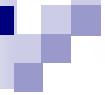
Доступ к сведениям, составляющим налоговую тайну, имеют должностные лица, определяемые соответственно федеральным органом исполнительной власти, уполномоченным по контролю и надзору в области налогов и сборов, федеральным органом исполнительной власти, уполномоченным в области внутренних дел, федеральным государственным органом, осуществляющим полномочия в сфере уголовного судопроизводства, федеральным органом исполнительной власти, уполномоченным в области таможенного дела. (п. 3 ст. 102).

Утрата документов, содержащих составляющие налоговую тайну сведения, либо разглашение таких сведений влечет ответственность, предусмотренную федеральными законами (п. 4 ст. 102).

## **За утрату документов** сотрудники налоговых органов несут дисциплинарную ответственность.

Согласно ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»:

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, обмана, шантажа, принуждения, подкупа или угроз, а равно иным незаконным способом - **наказывается** штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок **до двух лет**, либо лишением свободы на тот же срок.



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 одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок **до четырех лет**, либо лишением свободы на тот же срок.

3. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -  
**наказываются** штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо принудительными работами на срок **до пяти лет**, либо лишением свободы на тот же срок.
4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, -  
**наказываются** принудительными работами на срок до пяти лет либо лишением свободы на срок **до семи лет**.

**К материальным носителям** сведений содержащим служебную, ГТ или КТ относятся: **бумага, магнитная лента, физические поля, фото- и кинопленка, дискеты, 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** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду (п.1, ст. 3 «Основные понятия, используемые в настоящем Федеральном законе» ФЗ «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ).

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п.1, ст. 3 «Основные понятия, используемые в настоящем Федеральном законе» ФЗ «О персональных данных» от 27.07.2006 г. № 152-ФЗ.

**Служебная информация (ограниченного доступа) –**  
информация, касающаяся деятельности организации, не являющаяся общедоступной и ограничение на распространение которой диктуется служебной необходимостью.

Доступ к служебной информации может быть ограничен ее обладателем в рамках реализации полномочий, предусмотренных ч.3 ст. 6 ФЗ от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Ограничение доступа к сведениям в режиме служебной информации представляется целесообразным в том случае, когда указанные сведения не составляют иную охраняемую законом тайну - государственную, коммерческую, служебную (в отношении сведений, полученных в рамках служебных правоотношений в их публично-правовом смысле) и т.д.

**Профессиональная тайна** – это защищаемая законом информация, доверенная или ставшая известной лицу (держателю информации) исключительно в силу исполнения им профессиональных обязанностей, не связанная с государственной или муниципальной службой. Определяется тремя признаками:

- профессиональная принадлежность;
- конфиденциальная информация добровольно доверяется лицу, исполняющему соответствующие профессиональные обязанности, по выбору владельца этой информации;
- у лица, к которому поступает такая информация, возникает обязанность обеспечить ее сохранность.

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

- определил **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**.

Обладатель информации, составляющей коммерческую тайну, имеет право защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав (ст. 6.1. «Права обладателя информации, составляющей коммерческую тайну» ФЗ «О коммерческой тайне»).

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 также незаконные оказание ему услуг имущественного характера, предоставление иных имущественных прав (в том числе когда по указанию такого лица имущество передается, или услуги имущественного характера оказываются, или имущественные права предоставляются иному физическому или юридическому лицу) за совершение действий (бездействие) в интересах дающего или иных лиц, если указанные действия (бездействие) входят в служебные полномочия такого лица либо если оно в силу своего служебного положения может способствовать указанным действиям (бездействию), -**

**наказываются штрафом в размере до четырехсот тысяч рублей, или в размере заработной платы или иного дохода осужденного за период до шести месяцев, или в размере от пятикратной до двадцатикратной суммы коммерческого подкупа, либо ограничением свободы на срок до двух лет, либо исправительными работами на срок до двух лет, либо лишением свободы на тот же срок со штрафом в размере до пятикратной суммы коммерческого подкупа или без такового.**

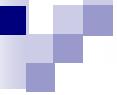
2. Деяния, предусмотренные частью первой настоящей статьи, совершенные в значительном размере, - **наказываются штрафом в размере до восьмисот тысяч рублей**, или в размере заработной платы или иного дохода осужденного за период до девяти месяцев, или в размере от десятикратной до тридцатикратной суммы коммерческого подкупа с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового, либо ограничением свободы на срок от одного года до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо исправительными работами на срок от одного года до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок **до трех лет** со штрафом в размере до десятикратной суммы коммерческого подкупа или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные ч. 1 настоящей статьи, если они совершены:
- а) группой лиц по предварительному сговору или организованной группой;
  - б) за заведомо незаконные действия (бездействие);
  - в) в крупном размере, -

**наказываются** штрафом в размере **до одного миллиона пятисот тысяч рублей**, или в размере заработной платы или иного дохода осужденного за период до одного года, или в размере от двадцатикратной до пятидесятикратной суммы коммерческого подкупа с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок от трех **до семи лет** со штрафом в размере до тридцатикратной суммы коммерческого подкупа или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

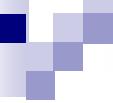
4. Деяния, предусмотренные ч. 1, п. "а" и "б" ч. 3 настоящей статьи, совершенные в особо крупном размере, - **наказываются** штрафом в размере от одного миллиона **до двух миллионов пятисот тысяч рублей**, или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет шести месяцев, или в размере от сорокакратной до семидесятикратной суммы коммерческого подкупа с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового либо лишением свободы на срок от четырех **до восьми лет** со штрафом в размере до сорокакратной суммы коммерческого подкупа или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

5. Незаконное получение лицом, выполняющим управленческие функции в коммерческой или иной организации, денег, ценных бумаг, иного имущества, а также незаконное пользование им услугами имущественного характера или иными имущественными правами (в том числе когда по указанию такого лица имущество передается, или услуги имущественного характера оказываются, или имущественные права предоставляются иному физическому или юридическому лицу) за совершение действий (бездействие) в интересах дающего или иных лиц, если указанные действия (бездействие) входят в служебные полномочия такого лица либо если оно в силу своего служебного положения может способствовать указанным действиям (бездействию), - **наказываются штрафом в размере до семисот тысяч рублей, или в размере заработной платы или иного дохода осужденного за период до девяти месяцев, или в размере от десятикратной до тридцатикратной суммы коммерческого подкупа либо лишением свободы на срок до трех лет со штрафом в размере до пятнадцатикратной суммы коммерческого подкупа или без такового.**



6. Деяния, предусмотренные ч. 5 настоящей статьи, совершенные в значительном размере, -

**наказываются штрафом в размере от двухсот тысяч до одного миллиона рублей**, или в размере заработной платы или иного дохода осужденного за период от трех месяцев до одного года, или в размере от двадцатикратной до сорокакратной суммы коммерческого подкупа с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок **до пяти лет** со штрафом в размере до двадцатикратной суммы коммерческого подкупа или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.



7. Деяния, предусмотренные ч. 5 настоящей статьи, если они:

а) совершены группой лиц по предварительному сговору или организованной группой;

б) сопряжены с вымогательством предмета подкупа;

в) совершены за незаконные действия (бездействие);

г) совершены в крупном размере, -

**наказываются штрафом в размере от одного миллиона до трех миллионов рублей**, или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, или в размере от тридцатикратной до шестидесятикратной суммы коммерческого подкупа с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет либо лишением свободы на срок от пяти **до девяти лет** со штрафом в размере до сорокакратной суммы коммерческого подкупа или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

8. Деяния, предусмотренные ч. 5, п. "а" - "в" ч. 7 настоящей статьи, совершенные в особо крупном размере, - **наказываются штрафом в размере от двух миллионов до пяти миллионов рублей**, или в размере заработной платы или иного дохода осужденного за период от двух до пяти лет, или в размере от пятидесятикратной до девяностократной суммы коммерческого подкупа с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет либо лишением свободы на срок от семи **до двенадцати лет** со штрафом в размере до пятидесятикратной суммы коммерческого подкупа или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет или без такового.

**Примечание 1. Значительным размером коммерческого подкупа в настоящей статье и статье 204.1 настоящего Кодекса признаются сумма денег, стоимость ценных бумаг, иного имущества, услуг имущественного характера, иных имущественных прав, превышающие двадцать пять тысяч рублей, крупным размером коммерческого подкупа - превышающие сто пятьдесят тысяч рублей, особо крупным размером коммерческого подкупа - превышающие один миллион рублей.**

**Примечание 2.** Лицо, совершившее преступление, предусмотренное ч. 1 - 4 настоящей статьи, освобождается от уголовной ответственности, если оно активно способствовало раскрытию и (или) расследованию преступления и либо в отношении его имело место вымогательство предмета подкупа, либо это лицо добровольно сообщило о совершенном преступлении в орган, имеющий право возбудить уголовное дело.

## УК РФ Статья 187. Неправомерный оборот средств платежей

1. Изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт поддельных платежных карт, распоряжений о переводе денежных средств, документов или средств оплаты (за исключением случаев, предусмотренных статьей 186 настоящего Кодекса), а также электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств, -

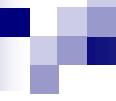
**наказываются** принудительными работами на срок до пяти лет либо лишением свободы на срок **до шести лет** со штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.



2. Те же деяния, совершенные организованной группой, - **наказываются** принудительными работами на срок до пяти лет либо лишением свободы на срок **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 или 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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич**  
**Некрасов Алексей Валентинович**

## **Вопросы к подразделам 8.1, 8.2 и 8.3**

- 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)



Под **персональными данными (ПД)** понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ "О персональных данных" от 27.07.2006 г. № 152-ФЗ. По сути, это всевозможные сведения, с помощью которых можно определить (идентифицировать) субъекта персональных данных, что в полной мере согласуется с положениями ст. 2 «Конвенции о защите физических лиц при автоматизированной обработке персональных данных», принятой Советом Европы 28 января 1981 г. Правовой защите подлежит лишь та информация о человеке, которая позволяет его персонифицировать. Схожее определение персональных данных приводится и в Регламенте Европейского Парламента и Совета Европейского Союза 2016/679 от 27.04.2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR) То есть и ФЗ "О персональных данных" и европейский Регламент определяют персональные данные достаточно широко, поэтому какого-либо перечня сведений, относящихся к персональным данным субъекта, не существует.

**Исторически необходимость принятия мер по защите ПД была вызвана двумя факторами:**

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

**Согласно данным компании Perimetrix, утечки данных определяются 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%).**

**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).**

**Самыми «популярными» персональными данными среди инсайдеров являются:**  
**детали конкретных сделок (47%),**  
**финансовые отчеты (38%),**  
**интеллектуальная собственность компании (25%),**  
**бизнес-планы (19%),**  
**прочие информационные ресурсы (14%).**

**Каналы утечки данных распределились так:**

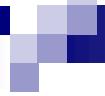
- 1. Мобильные накопители – 74%**
- 2. Электронная почта – 58%**
- 3. Интернет-мессенджеры – 17%**
- 4. Интернет (web-почта, форумы, блоги) – 26%**
- 5. Принтеры – 18%**
- 6. Фото-видео-устройства – 2%**
- 7. Другие – 5%**

**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.**

**ПД из ЕС 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 «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19.12.2005 г. № 160-ФЗ), тормозило обмен сведениями с европейскими государственными и компаниями, делая невозможными многие коммерчески перспективные проекты.**



**ФЗ «О персональных данных» от 27.07.2006 г. № 152-ФЗ 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:**

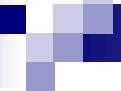
- защита ПД от НСД к ним со стороны других лиц, в том числе представителей государственных органов и служб, не имеющих на то необходимых полномочий;**
- обеспечение сохранности, целостности и достоверности данных в процессе работы с ними, в том числе при передаче по каналам связи;**

- 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 изменилась работа с документами, содержащими ПД.**

1. Во всех организациях появился 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. Возникла **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. Установлен норматив **сроков хранения** документов и информации и максимальный срок хранения, который необходимо соблюдать и отслеживать.
  4. При работе с ПД **необходимо** заранее продумать и **зарегистрировать 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.

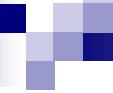
# **Участники правовых отношений**

**Закон распространяется на всех участников**

**(государственные, юридические и физические лица) (ст. 1).**

1. Им регулируются отношения, связанные с обработкой персональных данных, осуществляющей федеральными органами государственной власти, органами государственной власти субъектов РФ, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

1. Положения настоящего ФЗ применяются к обработке персональных данных граждан РФ, осуществляющей иностранными юридическими лицами или иностранными физическими лицами, на основании договора, стороной которого являются граждане РФ, иных соглашений между иностранными юридическими лицами, иностранными физическими лицами и гражданами РФ либо на основании согласия гражданина РФ на обработку его персональных данных.
2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:
  - 1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
  - 2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда РФ и других архивных документов в соответствии с законодательством об архивном деле в РФ;
  - 4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.



3. Предоставление, распространение, передача и получение информации о деятельности судов в Российской Федерации, содержащей персональные данные, ведение и использование информационных систем и информационно-телекоммуникационных сетей в целях создания условий для доступа к указанной информации осуществляются в соответствии с ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации" от 22.12.2008 г. № 262-ФЗ.

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну (ст. 2).

В целях настоящего ФЗ используются следующие основные понятия (ст. 3):

- 1) **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 1\_1) **персональные данные, разрешенные субъектом персональных данных для распространения**, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;
- 2) **оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

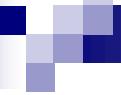
- 3) обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- 4) автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;
- 5) распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 6) предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 7) блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- 8) уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- 9) обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 10) информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 11) трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

## **Принципы обработки персональных данных (ст. 5).**

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

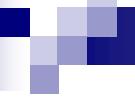


## Условия обработки персональных данных (ст. 6).

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим ФЗ.  
Обработка персональных данных допускается в следующих случаях:
  - 1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
  - 2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на оператора функций, полномочий и обязанностей;
  - 3) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
  - 3\_1) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);



4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов РФ, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных ФЗ от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

- 
- 5) обработка персональных данных необходима для исполнения договора, стороны которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством РФ, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;
  - 6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- 7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных ФЗ "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в ФЗ "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- 8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
- 9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего ФЗ, при условии обязательного обезличивания персональных данных;

- 9\_1) обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24.04.2020 г. № 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте РФ - городе федерального значения Москве и внесении изменений в статьи 6 и 10 ФЗ "О персональных данных" и ФЗ от 31 июля 2020 года № 258-ФЗ "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации", в порядке и на условиях, которые предусмотрены указанными федеральными законами;
- 11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
- 1\_1. Обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных ФЗ от 27.05.1996 г. № 57-ФЗ "О государственной охране".

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего ФЗ.
3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим ФЗ, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных настоящим ФЗ. В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных

данных, требования, предусмотренные ч. 5 ст. 18 и ст. 18\_1 настоящего ФЗ, обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 настоящего ФЗ, в том числе требование об уведомлении оператора о случаях, предусмотренных ч. 3\_1 ст. 21 настоящего ФЗ.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.
5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

6. В случае, если оператор поручает обработку персональных данных иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом персональных данных за действия указанных лиц несет оператор и лицо, осуществляющее обработку персональных данных по поручению оператора.

### **Конфиденциальность персональных данных (ст. 7).**

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Ст. 8 устанавливает порядок включения (исключения) персональных данных в общедоступные источники (из общедоступных источников) персональных данных (в том числе справочники, адресные книги).

Ст. 9 устанавливает нормы, связанные с получением и отзывом согласия субъекта персональных данных на обработку его персональных данных, а также определяет, что должно включать в себя это согласие.

## **Согласие субъекта персональных данных на обработку его персональных данных (ст. 9).**

Ст. 9 устанавливает нормы, связанные с получением и отзывом согласия субъекта персональных данных на обработку его персональных данных, а также определяет, что должно включать в себя это согласие.

4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных (если он его представляет), номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя;
- 3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- 4) цель обработки персональных данных;
- 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- 8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- 9) подпись субъекта персональных данных.

**Выделяется 2 способа обработки ПД:**

- с использованием средств автоматизации;**
- без использования средств автоматизации.**

Такое же понимание можно найти в нормативных актах Роскомнадзора.

Под **автоматизированным способом обработки ПД** законодатель и ведомство понимают совершение любых действий с персональными данными, которые связаны с использованием средств вычислительной техники. Закон не раскрывает термин «средства вычислительной техники» конкретно, но очевидно, что под ними понимаются информационные системы. Для способа обработки персональных данных средствами автоматизации есть одно серьезное ограничение. Ни одно решение, на основании которого могут быть изменены права или обязанности гражданина, не может быть принято только исходя из результатов обработки сведений средствами вычислительной техники.

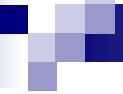
**Ручной (не автоматизированный) способ обработки ПД** – это занесение их на материальные носители вручную и дальнейшая работа с такими носителями.

Закон в дальнейшем не конкретизирует особенности организации работы каждым способом, предоставляя это сделать ФСТЭК России. Ведомство, в свою очередь, определяет требования к автоматизированному способу обработки и используемым для него средствам. С точки зрения ручного способа действуют или общие принципы, или организационные меры, затрудняющие физический доступ к персональным данным путем разграничения функционала сотрудников. Так же необходимо выполнять требования по физической защите помещений.

Закон «О персональных данных» называет несколько видов действий, которые могут производиться с поступившими в распоряжение организации персональными данными. Этот перечень ограничен и расширительному толкованию не подлежит. Таким образом, оператор ПД может производить с ними следующие действия:

- **сбор** – это фактическая передача ПД от их субъекта оператору;
- **запись** – может происходить и ручным, и машинным способом;
- **систематизация** – техническое действие, облегчающее обработку ПД для оператора;
- **накопление** – термин не имеет самостоятельного значения и предполагает хранение информационных массивов на материальных носителях или с использованием средств автоматизации до момента их уничтожения;
- **хранение** – законодатель устанавливает множество требований к способам физической и технической защиты ПД;
- **уточнение** – под этим термином могут подразумеваться или обновление, или изменение информации;
- **извлечение** – здесь предполагается перенос ПД из памяти средств автоматизации на материальные носители;
- **использование** – действия (операции) с ПД, совершаемые оператором в определенных целях;

- **передача** – термин рассматривает такие способы предоставления к данным доступа третьим лицам, как распространение, предоставление. **Распространение** предполагает, что сведения становятся доступными неограниченному кругу лиц, которые могут получить их, зайдя на открытый сайт, купив газету или компакт-диск с информацией. Для **предоставления** характерно совершение тех же действий, но в отношении нескольких субъектов, определенных соглашением или иным способом;
- **обезличивание** – действия, в результате которых невозможно определить принадлежность ПД конкретному субъекту. Обезличивание может происходить только в условиях применения способа обработки данных при помощи средств автоматизации. Если оно используется, выделение данных одного субъекта из массива возможно только при применении специальных средств;
- **блокирование** – временное прекращение любых действий с ПД. Блокировка производится по заявлению субъекта персональных данных или по требованию регулятора. Если она необходима, обработка сведений возможна только в целях их уточнения;



- **удаление** – отличается от уничтожения, так как производится в целях коррекции ПД или для решения иных технических задач;
- **уничтожение** – действия, которые не только уничтожают ПД, обрабатываемые ручным или автоматизированным способом, но и полностью исключают их восстановление. Если данные находились на материальных носителях, вместе с ними уничтожаются и сами носители. Уничтожение происходит по требованию субъекта ПД или по истечении срока их обработки.

## Виды персональных данных

Поскольку законодатель не приводит какого-либо перечня сведений, относимых к категории ПД, исходя из особенностей обработки отдельных категорий ПД можно выделить следующие их группы.

1. **Обычные ПД**, то есть это те сведения о физическом лице, которые не являются специальными ПД (ст. 10 ФЗ № 152-ФЗ); биометрическими ПД (ст. 11 ФЗ № 152-ФЗ); данными, разрешенными субъектом для распространения (ст. 10\_1 ФЗ № 152-ФЗ).

К категории обычных ПД могут быть отнесены так называемые "анкетные" данные гражданина (ФИО, образование, место жительства и др.). То есть это те сведения, которые сообщаются самим субъектом персональных данных (п. 1 ст. 8 ФЗ № 152-ФЗ).

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (различные справочники, адресные книги и т. п.). При этом по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов персональные данные должны быть исключены из подобных источников (п. 2 ст. 8 ФЗ № 152-ФЗ).

Режим конфиденциальности информации не распространяется также в случаи обезличивания ПД или совершения действий, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (п. 9 ст. 3 ФЗ № 152-ФЗ).

**2. Персональные данные, разрешенные субъектом ПД для распространения** (далее – разрешенные ПД). К ним относятся сведения, доступ неограниченного круга лиц к которым предоставлен субъектом ПД путем дачи отдельного письменного согласия на обработку персональных данных (п. 1\_1 ст. 3 ФЗ № 152-ФЗ). Требования к содержанию такого согласия утверждены приказом Роскомнадзора от 24.02.2021 г. № 18 (действуют до 1 сентября 2027 года). Особенности обработки таких данных урегулированы ст. 10\_1 ФЗ № 152-ФЗ.

Согласие субъекта ПД выступает в качестве исключительного правового основания на обработку разрешенных ПД, содержание которого в обязательном порядке должно включать в себя перечень ресурсов оператора, на которых планируется размещать эти сведения. Оператор обязан обеспечить субъекту ПД возможность определить перечень разрешенных персональных данных по каждой категории, указанной в согласии.

В целях обеспечения реализации принципа волеизъявления субъекта ПД введены положения, не допускающие получение оператором согласия по умолчанию или бездействию субъекта ПД.

Вводится право субъекта ПД установить запрет на осуществление неограниченным кругом лиц обработки его разрешенных ПД (кроме получения доступа) и условия такой обработки и обязанность оператора информировать указанных лиц об имеющихся условиях и запретах.

**3. Специальные категории ПД** включают информацию о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждений, состояния здоровья, интимной жизни, о судимости и т. п. (п. 1 ст. 10 ФЗ № 152-ФЗ). Данный перечень не является закрытым и может дополняться новыми основаниями.

Придание специальным категориям ПД особого статуса обусловлено возможностью наступления крайне негативных последствий для человека при их противоправном распространении или ином несанкционированном использовании, которые могут выражаться в дискриминации носителя по различным признакам, невозможности реализации им статусных прав на образование, вероисповедание, проведение собраний и т.п.

**4. Биометрические ПД** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных (п. 1 ст. 11 ФЗ № 152-ФЗ).

В основе сбора и анализа сведений, составляющих биометрические данные человека, лежит использование биометрических признаков. Примерами биометрических методов идентификации являются дактилоскопические данные, изображение радужной оболочки глаз, анализы ДНК, изображение человека и др. Отметим, что с 08.05.2023 г. геномная информация также отнесена к биометрическим персональным данным.

Отнесение сведений персонального характера к биометрическим ПД и их последующая обработка должны рассматриваться в рамках проводимых оператором мероприятий, направленных на установление личности конкретного лица, если иное не предусмотрено федеральными законами и принятыми на их основе нормативными правовыми актами.

- Минцифры России в своем письме от 28.08.2020 г. № ЛБ-С-074-24059 указывало, что к биометрическим персональным данным не относятся:
- данные, полученные при сканировании паспорта оператором ПД для подтверждения осуществления определенных действий конкретным лицом (например, заключение договора на оказание услуг, в том числе банковских, медицинских и т. п.), т. е. без проведения процедур идентификации (установления личности);
  - данные, полученные при осуществлении ксерокопирования документа, удостоверяющего личность;
  - фотографическое изображение, содержащееся в личном деле работника;
  - подпись лица, являющейся обязательным требованием в различных договорных отношениях, и почерк, в том числе анализируемый уполномоченными органами в рамках почерковедческой экспертизы;
  - рентгеновские или флюорографические снимки, характеризующие физиологические и биологические особенности человека и находящиеся в истории болезни (медицинской карте) пациента (не имеет значения, бумажной или электронной), поскольку они не используются оператором (медицинским учреждением) для установления личности пациента;
  - материалы видеосъемки в публичных местах и на охраняемой территории. <https://www.garant.ru/actual/persona/>

**Правила обработки и обеспечения конфиденциальности ПД, собственных работников и сторонних физических лиц, ПД которых обрабатываются в организации, установлены:**

**Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».**

**Главой 14 Трудового Кодекса Российской Федерации от 30.12.2001 г. № 197-ФЗ.**

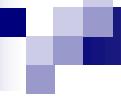
**ПП РФ "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" от 01.11.2012 г. № 1119.**

**ПП РФ "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" от 15.09.2008 г. № 687.**

**Нормативными документами ФСБ и ФСТЭК.**

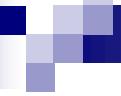
**Персональными данными гражданина, подлежащим защите, признается любая информация, относящаяся к физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.**

**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.**



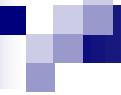
**Обмен персональными данными при их обработке в информационных системах осуществляется по защищенным каналам связи.**

**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 может 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.

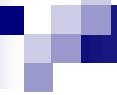
Необходимо обеспечивать раздельное хранение ПД (материальных носителей), обработка которых осуществляется в различных целях.

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.**

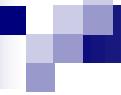
**Возможны также гражданские иски к организации, принудительное приостановление или прекращение обработки ПД в организации, приостановление действия или аннулирование лицензий.**



**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.

**Основные положения из:**

**ПП РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 от 01.11.2012 г.**

**Приказ ФСТЭК «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» № 21 от 18.02.2013 г.**

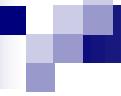
**Постановлением Правительства РФ № 1119**

- 1. Даны уточнения определения ИС ПД в зависимости от категорий ПД.**
- 2. Установлены 4 уровня защищенности ПД при их обработке в информационных системах.**

**5. ИС является информационной системой, обрабатывающей специальные категории ПД**, если в ней обрабатываются ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПД.

**ИС является информационной системой, обрабатывающей биометрические ПД**, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПД, и не обрабатываются сведения, относящиеся к специальным категориям ПД.

**ИС является информационной системой, обрабатывающей общедоступные ПД**, если в ней обрабатываются ПД субъектов ПД, полученные только из общедоступных источников ПД, созданных в соответствии со ст. 8 ФЗ "О персональных данных".



ИС является **информационной системой, обрабатывающей иные категории ПД**, если в ней не обрабатываются ПД, указанные в абзацах 1 – 3 настоящего пункта.

ИС является **информационной системой, обрабатывающей ПД сотрудников оператора**, если в ней обрабатываются ПД только указанных сотрудников. В остальных случаях ИС ПД является **информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора**.

В соответствии с ПП № 1119 оператору или лицу, осуществляющему обработку ПД по поручению оператора на основании заключаемого с этим лицом договора, необходимо создать систему защиты ПД, обеспечивающую безопасность ПД, включающую организационные и (или) технические меры, которые определяются с учетом:

- актуальных угроз безопасности персональных данных;
- информационных технологий, используемых в ИС ПД (ИСПДн).

В ПП № 1119 установлены как новые требования к операторам, так и требования, ранее закрепленные в других нормативных правовых актах:

1. Необходимо включить в договор между оператором и уполномоченным лицом обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в ИСПДн (Данный пункт необходим к исполнению в случае, если соответствующие положения еще не закреплены в договорах с уполномоченными лицами во исполнение ч. 3 ст. 6 152-ФЗ.).

2. СЗИ для системы защиты ПД должны быть выбраны оператором в соответствии с действующими нормативными правовыми актами ФСБ России и ФСТЭК России во исполнение ч. 4 ст. 19 152-ФЗ.

3. Необходимо определить, какие категории персональных данных обрабатываются в каждой ИСПДн, а также к какой из двух категорий субъектов (работники оператора или иные лица) принадлежат эти персональные данные:

- специальные категории персональных данных;
- биометрические персональные данные;
- общедоступные персональные данные;
- иные категории персональных данных.

При этом:

- в ПП № 1119 не упоминаются обезличенные персональные данные как категория персональных данных. Следовательно, для персональных данных, в отношении которых были совершены действия по обезличиванию, определение уровня защищенности не требуется;

- сведения о судимости не причислены ни к одной из вышеназванных категорий ПД, несмотря на то, что в ст. 10 ФЗ № 152-ФЗ они отнесены к специальным категориям;
- ИСПДн признается обрабатывающей общедоступные ПД, если в ней обрабатываются ПД субъектов, полученные только из общедоступных источников ПД. Случаи, когда персональные данные сделаны субъектом общедоступными в соответствии с п.10 ч.1 ст.6 152-ФЗ, в ПП № 1119 не рассмотрены.

4. Необходимо определить, угрозы какого типа из трех возможных актуальны для этих ИСПДн в зависимости от наличия недокументированных (недекларированных) возможностей, а также типа программного обеспечения (системное (далее - СПО) или прикладное (далее – ППО)). Определение типа актуальных угроз должно осуществляться с учетом оценки возможного вреда субъектам ПД и в соответствии с нормативными правовыми актами, определяющими актуальные угрозы безопасности ПД при их обработке в ИСПДн при осуществлении соответствующих видов деятельности.

В ст. 6. ФЗ № 152-ФЗ под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПД при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

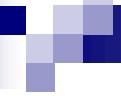
Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

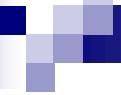
(К угрозам 1-го типа относятся комбинации факторов и условий, обусловленные наличием НДВ в системном, а иногда и в прикладном софте информационной системы ПДн. То есть используемые аппаратные возможности и утилиты могут стать причиной неправомерной блокировки, изменения, удаления и распространения личных сведений граждан.

Угрозы 2-го типа выявляются в системах, где есть недекларируемые возможности в применяемых прикладных программах. Например, утилита, которая собирает и систематизирует ПДн, может быть использована для несанкционированного внесения изменений или уничтожения информации.

Угрозы 3-го типа - Наиболее удачный вариант в плане затрат на защиту ИСПДн, когда отсутствует опасность получения доступа к персональным данным со стороны сотрудников и третьих лиц вследствие наличия НДВ в программном обеспечении.)



5. Необходимо разработать документ, на основании которого можно оценить возможный вред субъектам персональных данных в случае нарушения ФЗ № 152-ФЗ (Данный пункт необходим к исполнению в случае, если оценка вреда субъектам ПД еще не произведена оператором во исполнение п. 5 ч. 1 ст. 18\_1 ФЗ № 152-ФЗ.).
6. Необходимо установить количество субъектов, ПД которых обрабатываются в каждой ИСПДн (больше 100 000 или меньше 100 000).
7. Необходимо определить, какой уровень защищенности ПД из четырех возможных необходимо обеспечивать при их обработке в ИСПДн (Таблица 1) на основании:
  - типа актуальных угроз;
  - категорий ПД, обрабатываемых в ИСПДн;
  - категорий субъектов, ПД которых обрабатываются в ИСПДн;
  - количества субъектов, ПД которых обрабатываются в каждой ИСПДн.



8. Выполнить требования, предусмотренные в ПП № 1119, для обеспечения соответствующего уровня защищенности ПД (Таблица 2). Самый низкий УЗ – четвертый, самый высокий – первый.

<https://fstec21.blogspot.com/2017/07/the-level-of-protection-of-personal-data.html>

9. Оператору (уполномоченному лицу) необходимо не реже 1 раза в 3 года организовывать и проводить контроль за выполнением указанных требований (самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации).

<https://rppa.ru/analitika/pp1119>

**Таблица 1. Определение уровней защищенности (УЗ) персональных данных**

Категории ПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			I (НДВ в СПО)	II (НДВ в ППО)	III (нет НДВ)
Специальные	Нет	более 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	менее 100 000		УЗ-2	УЗ-3
	Да	–		УЗ-3	
Биометрические	–	–	УЗ-2	УЗ-3	УЗ-4
Общедоступные	Нет	более 100 000			
	Нет	менее 100 000		УЗ-3	
	Да	–			
Иные	Нет	более 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	менее 100 000		УЗ-3	УЗ-4
	Да	–			

**Таблица 2. Определение требований, выполнение которых необходимо для обеспечения соответствующих УЗ**

Требования	УЗ			
	1	2	3	4
Режим обеспечения безопасности помещений, где обрабатываются персональные данные	+	+	+	+
Сохранность носителей персональных данных	+	+	+	+
Перечень лиц, допущенных к персональным данным	+	+	+	+
СЗИ, прошедшие процедуру оценки соответствия	+	+	+	+
Должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн	+	+	+	–
Ограничение доступа к содержанию электронного журнала сообщений	+	+	–	–
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным	+	–	–	–
Структурное подразделение, ответственное за обеспечение безопасности персональных данных	+	–	–	–

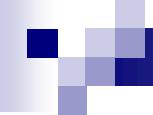
**Приказом ФСТЭК "Об утверждении Состава и  
содержания организационных и технических мер по  
обеспечению безопасности персональных данных  
при их обработке в информационных системах  
персональных данных" № 21 от 18.02.2013 г.**

**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.**

## **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.

## **Ответственность за нарушение требований ФЗ «О персональных данных» от 27.07.2006 г. № 152-ФЗ (ст. 24)**

1. Лица, виновные в нарушении требований настоящего ФЗ, несут предусмотренную законодательством РФ ответственность (распространяется на правоотношения, возникшие с 01.07.2011г.).
2. Моральный вред, причиненный субъекту ПД вследствие нарушения его прав, нарушения правил обработки ПД, установленных настоящим ФЗ, а также требований к защите ПД, установленных в соответствии с настоящим ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПД убытков (распространяется на правоотношения, возникшие с 01.07.2011 г.).

Лицам, нарушившим требования ФЗ № 152-ФЗ, в зависимости от конкретных обстоятельств и серьезности деяния может грозить не только административная и уголовная ответственность, но также гражданско-правовая и даже дисциплинарная.

<https://www.garant.ru/actual/persona/otvetstvennost/>

## **Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных**

Оценка вреда осуществляется в соответствии с требованиями, утв. приказом Роскомнадзора "Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных" от 27.10.2022 г. № 178.

## **Утечка персональных данных**

Согласно п. 10 ст. 23 ФЗ «О персональных данных», для учета информации об инцидентах, поименованных в п. 3.1 ст. 21 этого закона, Роскомнадзор ведет реестр учета инцидентов в области ПД. Приказом Роскомнадзора от 14.11.2022 г. № 187 установлен порядок и условия взаимодействия Роскомнадзора с операторами в рамках ведения названного реестра. В том числе этим приказом закреплены требования к содержанию первичного и дополнительного уведомления об инциденте.

## **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. Назовите мероприятия, проводимые по обеспечению безопасности ИС.**

# **Организационное и правовое обеспечение информационной безопасности**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**

## **Вопросы к подразделу 8.4**

- 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. 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. За общими критериями оценки безопасности информационных технологий закрепилось название **Общие критерии** (ОК).

Главная тенденция, которая прослеживается при анализе современных стандартов в области информационной безопасности, состоит в отказе от жесткой универсальной шкалы классов безопасности и обеспечении гибкости в подходе к оценке безопасности различных типов изделий ИТ.

#### **История создания данного стандарта**

В начале 80-х годов в США были разработаны "Критерии оценки доверенных компьютерных систем" (TCSEC – Trusted Computer System Evaluation Criteria) – стандарт Министерства обороны США, устанавливающий основные условия для оценки эффективности средств компьютерной безопасности, содержащихся в компьютерной системе. Критерии используются для определения, классификации и выбора компьютерных систем, предназначенных для обработки, хранения и поиска важной или секретной информации.

## **История создания стандарта**

В начале 80-х годов в США были разработаны "**Критерии оценки доверенных компьютерных систем**" (TCSEC – Trusted Computer System Evaluation Criteria) – стандарт Министерства обороны США, устанавливающий основные условия для оценки эффективности средств компьютерной безопасности, содержащихся в компьютерной системе, который еще называют «Оранжевой книги». Критерии используются для определения, классификации и выбора компьютерных систем, предназначенных для обработки, хранения и поиска важной или секретной информации.

В Европе в 1991 г. были разработаны "**Критерии оценки безопасности информационных технологий**" (ITSEC – Information Technology Security Evaluation Criteria) совместно Францией, Германией, Нидерландами и Великобританией.

В Канаде в начале 1993 г. были созданы "**Канадские критерии оценки доверенных компьютерных продуктов**" (CTCPEC - Canadian Trusted Computer Product Evaluation Criteria).

В США в это же время был издан проект стандарта "Федеральные критерии безопасности информационных технологий" (FC - Federal Criteria for Information Technology Security), 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**. В результате появился Международный стандарт ISO/IEC 15408-99 "Критерии оценки безопасности информационных технологий" или так называемые "Общие критерии" (ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security).

Появление «Общих критериев» оценки безопасности информационных технологий и соответствующих им международных стандартов явилось новым этапом в развитии нормативной базы оценки информационной безопасности.

## БАЗОВЫЕ ДОКУМЕНТЫ



Рис. 1. Предыстория «Общих критериев»

Аналогичный национарный стандарт был принят в России ГОСТ Р ИСО/МЭК 15408-1-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (принят постановлением Госстандарта РФ от 4 апреля 2002 г. № 133-ст) (отменен).

Действующим национальным стандартом является ГОСТ Р ИСО/МЭК 15408-1-2012 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814-ст).

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.

Действующим международным стандартом является ИСО/МЭК 15408-1:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model).

**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 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Меры обеспечения информационной безопасности» (ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls)

ГОСТ Р ИСО/МЭК 13335-1-2006 "Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий"

ГОСТ Р ИСО/МЭК 19794-2-2005 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки»

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

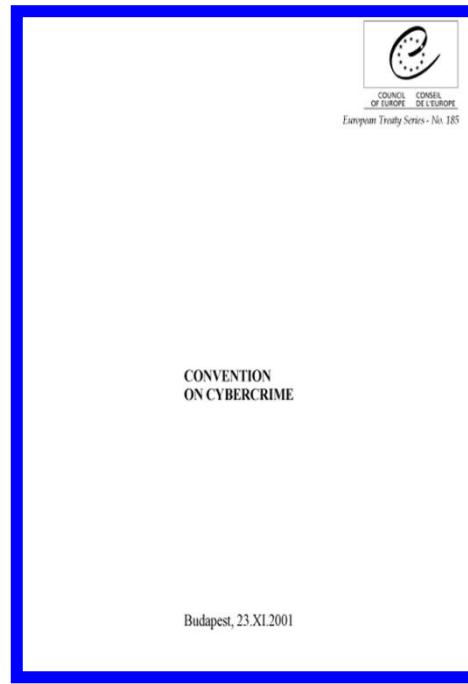
ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»

ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»

СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»

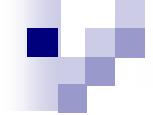
В Будапеште 23 ноября 2001 г. подписана **Конвенция по борьбе с киберпреступностью**. (26 европейских стран, а также Канады, США, ЮАР и Японии)



Конвенция разрабатывалась специальным комитетом Совета Европы при участии юристов США и других стран в течение 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 Стороны получать** через компьютерную систему на своей территории **доступ к хранящимся на территории другой стороны 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 несколько десятков стран, но далеко не все страны ее ратифицировали.**

## **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 по организации борьбы с противоправным  
использованием информационно-коммуникационных  
технологий МВД РФ (УБК МВД России)** (ранее Управление  
«К»).

<https://mvd.ru/mvd/structure1/Upravlenija/ubk>

Управление является самостоятельным структурным подразделением центрального аппарата Министерства внутренних дел Российской Федерации, обеспечивающим и осуществляющим в пределах компетенции функции МВД по выработке и реализации государственной политики и нормативно-правовому регулированию в области организации противодействия противоправным действиям, совершаемым с использованием (в сфере) информационно-коммуникационных технологий.

Среди основных задач Управления:

- предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере ИТ-технологий, а также координация этой деятельности в системе МВД России;
- анализ данных, содержащихся в информационно-телекоммуникационных сетях, в целях выявления запрещенного контента и противодействия преступности;
- организация взаимодействия подразделений ОВД РФ с государственными органами, органами государственной власти субъектов РФ, учреждениями финансово-кредитной системы, организациями информационно-коммуникационной сферы, иными участниками информационного обмена, включая агрегаторы больших данных.

Управление наблюдает за Рунет, закрывая незаконно действующие сайты.

Управлением 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:**

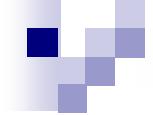
**чтобы утверждать, что было совершено**  
**преступление с использованием**  
**компьютера, необходимо доказать**  
**следующие факты:**



- компьютерная информация, к которой произведен **несанкционированный доступ**, охраняется законами РФ;
- злоумышленником были осуществлены определенные **неправомерные действия**;
- этими несанкционированными действиями **нарушены права собственника информации**;
- **несанкционированный доступ к средствам компьютерной техники** либо попытка доступа;
- **использование информации в преступных целях.**  
Например, с целью совершения преступления. Тогда **доказыванию подлежит**:
- совершение 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.

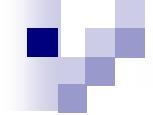
- 
4. **Допрос** инженеров, программистов и специалистов электронщиков, занимающихся эксплуатацией и ремонтов вычислительной техники.
  5. **Проведение комплексной судебно-бухгалтерской и программно-технической экспертизы** с привлечением соответствующих специалистов правоохранительных органов.

**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:**

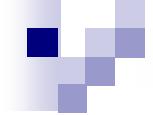
- "Жучок" (bugging) – установка микрофона в компьютере;
- "**Откачивание данных**" (data leakage) – возможность сбора информации, для получения данных, о технологии ее прохождения в системе;
- "**Уборка мусора**" (scavenging) – поиск данных, оставленных пользователем после работы на компьютере (в мусорных 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 "бреши" (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,ексуальные домогательства, кражу информации, внутригосударственный и международный терроризм, нарушение авторских прав, фальсификацию систем, насильственные преступления, жестокое обращение с пожилыми.**

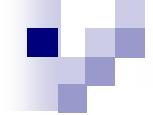
С целью совершенствования методов расследования, правоохранительные органы проводят **анализ КП**. **Создаются системы адаптации «традиционных» методов расследования преступлений с использованием компьютерных средств.**



**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 Компьютерная группа реагирования на чрезвычайные ситуации 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.

### **9.3. Требования к безопасности компьютерных сетей в РФ**

Эти требования были разработаны бывшей ГТК РФ и **обязательны для государственных предприятий или для коммерческих предприятий допущенных к сведениям составляющих ГТ**. В остальных случаях они носят рекомендательный характер.

Например, РД ГТК «**Автоматизированные системы. Защита от несанкционированного доступа к информации.**

**Классификация автоматизированных систем и требования по защите информации**» (утв. решением Государственной технической комиссии при Президенте РФ от 30.03.1992 г.) устанавливает классификацию АС, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

<https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodящий-dokument-ot-30-marta-1992-g-3>

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС – коллективный или индивидуальный.

**Требования к безопасности АС** устанавливаются в соответствии с классом защищенности. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Т.е. 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.

### Третья группа

АС, в которых работает **один пользователь**, допущенный **ко всей информации** АС, размещенной на носителях одного уровня конфиденциальности

#### 3 А

информация,  
составляющая гостайну

#### 3 Б

служебная тайна  
или персональные данные

### Вторая группа

АС, в которых **пользователи имеют одинаковые права доступа** (полномочия) **ко всей информации** АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности

#### 2 А

информация,  
составляющая гостайну

#### 2 Б

служебная тайна  
или персональные данные

### Первая группа

**многопользовательские** АС, в которых одновременно обрабатывается и/или хранится информация **разных уровней конфиденциальности** и **не все пользователи имеют право доступа ко всей информации** АС

#### 1 А

#### 1 Б

#### 1 В

#### 1 Г

#### 1 Д

АС, в которых циркулирует информация, составляющая гостайну:  
1А, 1Б и 1В.

**1 В** - в случае обработки секретной информации с грифом не выше «секретно»

**1 Б** - в случае обработки секретной информации с грифом не выше «совершенно секретно»

**1 А** - в случае обработки секретной информации с грифом «особая важность»

**1 Г** - АС, в которых циркулирует служебная тайна

**1 Д** - АС, в которых циркулируют персональные данные

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации.

Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Показатели защищенности средств вычислительной техники от НСД даны в РД ГТК «**Средства вычислительной техники. Защита от несанкционированного доступа к информации.** Показатели защищенности от несанкционированного доступа к информации» (утв. решением председателя Государственной технической комиссии при Президенте РФ от 30.03.1992 г.).

РД устанавливает классификацию средств вычислительной техники (СВТ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

В данном РД определяется 7 классов защищенности средств вычислительной техники (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.      |

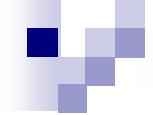
Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Применение в комплекте СВТ средств криптографической защиты информации может быть использовано для повышения гарантий качества защиты.

**Для присвоения класса защищенности АС должна иметь:**

- руководство администратора по системе;
- руководство пользователя;
- тестовую и конструкторскую документацию.

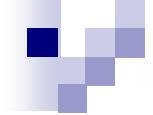
- Кроме этого действуют следующие РД ГТК:**
- "Защита от несанкционированного доступа к информации. Термины и определения"** (утв. решением председателя Гостехкомиссии России от 30.03.1992 г.)
- "Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации"** (утв. решением председателя Гостехкомиссии России от 30.03.1992 г.)
- "Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники"** (утв. решением председателя Гостехкомиссии России от 30.03.1992 г.)



**"Средства вычислительной техники. Межсетевые экраны.  
Защита от несанкционированного доступа к информации.  
Показатели защищенности от несанкционированного  
доступа к информации" (утв. решением председателя  
Гостехкомиссии России от 25.07.1997 г.)**

**«Защита информации. Специальные защитные знаки.  
Классификация и общие требования» (утв. решением  
председателя Гостехкомиссии России от 25.07.1997 г.)**

**"Специальные требования и рекомендации по технической  
защите конфиденциальной информации (СТР-К)" 2001 г.**



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),
- 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.**

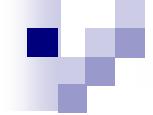
## **Политика безопасности имеет два-три уровня**

**Верхний уровень** политики безопасности 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 наличия 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** политики безопасности 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).**



## **9.4. 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:

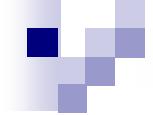
- **обеспечение уровня безопасности, соответствующего нормативным документам предприятия;**
- **достижение экономической целесообразности в выборе защитных мер;**
- **обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС.**

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"><li>- АС недостаточно защищены.</li><li>- Продолжительность вторжения сопряжена с финансовым риском.</li><li>- Неизвестен круг пользователей.</li><li>- Пользователей могут привлечь к ответственности за нанесенный ущерб и др.</li></ul>	<ul style="list-style-type: none"><li>- АС хорошо защищена, используются надежные средства резервирования.</li><li>- Имеют место повторяющиеся и частые атаки.</li><li>- Действия злоумышленника можно контролировать.</li><li>- Организация обладает положительным опытом работы с правоохранительными и правозащитными органами и др.</li></ul>



Для каждой категории пользователей указывается **правило пользования ресурсом** принятное в организации (выбирается из двух вариантов):

- что явно не запрещено, то разрешено;
- что явно не разрешено, то запрещено.

Утверждается **схема доступа** к сервисам:

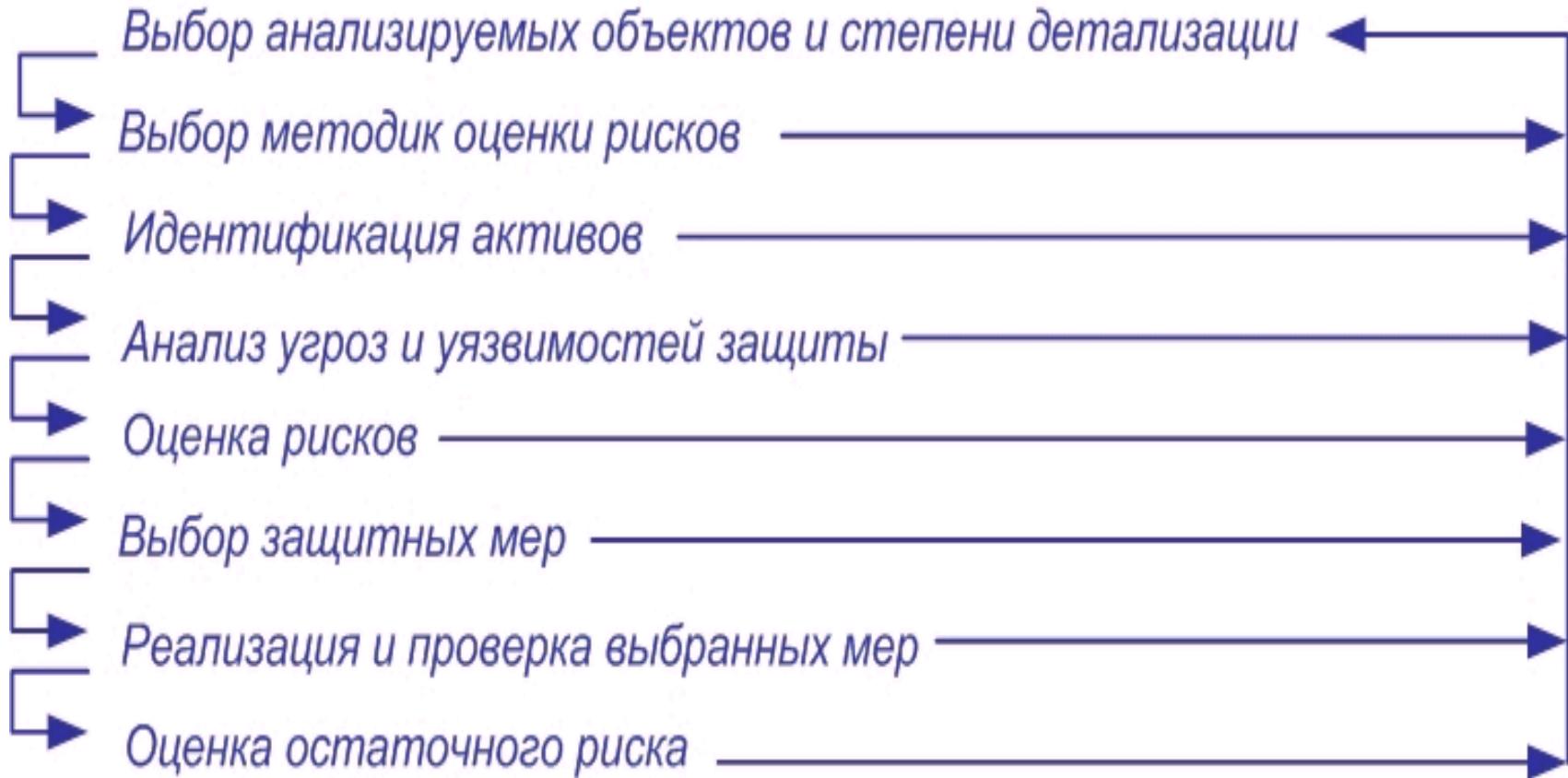
- централизованная;
- децентрализованная;
- иная.

## **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:**

$$E = V \cdot p,$$

где **p** – вероятность возникновения угрозы;  
**V** – оценка ущерба при реализации угрозы.

Если задан коэффициент защищенности СИБ (**K<sub>з</sub>**)  
(например, **K<sub>з</sub>** может быть 0,85 (85%), 0,9 (90%) и т.п.)

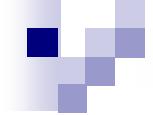
Тогда можно оценить величину ущерба при реализации  
угрозы используемым активам:

$$V = S \cdot (1 - K_{\text{з}}),$$

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 уровни 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 получились неприемлемы, то тогда повторяют этапы анализа риска.



## При создании системы безопасности 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.**

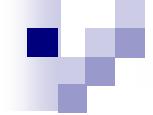
		Положение ЗЛ			
Объекты защиты	ЗЛ за пределами КЗ	ЗЛ в пределах контролируемой зоны (КЗ)			
		ЗЛ в пределах КЗ	ЗЛ в выделенном помещении	ЗЛ - сотрудник объекта	ЗЛ – сотрудник СБ
Человек	Гр. 4, 5, 7, 8	Гр. 5	Гр. 5	Гр. 5	Гр. 5
Информация	Гр. 3, 8, 9	Гр. 3, 6, 9	Гр. 3, 6, 9	Гр. 3, 6, 9	Гр. 3, 6, 9
Материаль-ные ценности	Гр. 1, 8	Гр. 1, 2	Гр. 1, 2	Гр. 1, 2	Гр. 1, 2



**Защита 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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**



## 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.

## **10. Защита интеллектуальной собственности**

### **10.1. Объекты интеллектуальной собственности**

П. 1 ст. 44 Конституции РФ устанавливает гарантии свободы творчества и охраны интеллектуальной собственности:

1. Каждому гарантировается свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

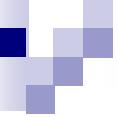
Термин **интеллектуальная собственность** в широком понимании означает закрепленное законом временное исключительное право, а также личные неимущественные права авторов на результат интеллектуальной деятельности или средства индивидуализации.

Законодательство, определяющее права на интеллектуальную собственность, устанавливает монополию авторов на определенные формы использования результатов своей интеллектуальной, творческой деятельности, которые, таким образом, могут использоваться другими лицами лишь с разрешения первых.

В ст. 1225 ГК РФ «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации» дается определение результатов интеллектуальной деятельности.

1. 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;

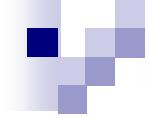


- 8) полезные модели;
  - 9) промышленные образцы;
  - 10) селекционные достижения;
  - 11) топологии интегральных микросхем;
  - 12) секреты производства (ноу-хау);
  - 13) фирменные наименования;
  - 14) товарные знаки и знаки обслуживания;
  - 14.1) географические указания;
  - 15) наименования мест происхождения товаров;
  - 16) коммерческие обозначения.
2. Интеллектуальная собственность охраняется законом.



## Ст. 1226 ГК РФ Интеллектуальные права

На результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (результаты интеллектуальной деятельности и средства индивидуализации) признаются интеллектуальные права, которые включают **исключительное право**, являющееся имущественным правом, а в случаях, предусмотренных настоящим Кодексом, также **личные неимущественные права и иные права** (право следования, право доступа и другие).



Существует три общепризнанные в мире правовые формы защиты объектов интеллектуальной собственности (ОИС):

- авторское право;
- патентное право;
- 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 сведений (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 1474 г. Изобретатель получал привилегию (патент) на 10 лет.

**В России** выдача привилегий началась с 1748 г. 17(29) июня 1812 г. был подписан Манифест «О привилегиях на разные изобретения и открытия в ремеслах и художествах» – первый патентный закон в России.

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 09.07.1993 г. № 5351-1 (утратил силу)
2. Закон РФ “**Патентный закон РФ**”, от 23.09.1992 г. № 3517-1 (утратил силу)
3. Закон РФ “**О правовой охране программ для ЭВМ и баз данных**”, от 23.09.1992 г. № 3523-1 (утратил силу)
4. Закон РФ “**О правовой охране топологии интегральных микросхем**”, от 23.09.1992 г. № 3526-1 (утратил силу)
5. Закон РФ “**О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров**”, от 23.09.1992 г. № 3520-1 (утратил силу)
6. Закон РСФСР “**О конкуренции и ограничении monopolisticheskoy deyatelnosti na tovarnyx rynkax**”, от 22.03.1991 г. № 948-1.
7. Закон РФ "О защите конкуренции", от 26.07.2006 г. № 135-ФЗ.



После вступления в силу с 01.01.2008 г. 4-й части Гражданского кодекса РФ большинство указанных выше законов, касающихся защиты ИС, потеряло силу.

**Заключены следующие международные конвенции и соглашения, связанные с охраной интеллектуальной собственности:**

- 1. Конвенция по охране промышленной собственности** от 20.03.1883 г. (редакция от 02.10.1979 г.), заключенная в Париже.
- 2. Бернская Конвенция по охране литературных и художественных произведений** от 09.09.1886 г. (редакция от 28.09.1979 г.).



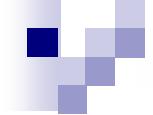
- 3. Мадридское соглашение о международной регистрации знаков от 14.04.1891 г. (редакция 02.10.1979 г.).**
- 4. Всемирная конвенция об авторском праве от 06.09.1952 г., заключенная в Женеве.**
- 5. Конвенция по охране интересов производителей фонограмм от незаконного воспроизведения фонограмм от 29.10.1971 г., заключенная в Женеве.**
- 6. Конвенция, учреждающая Всемирную Организацию Интеллектуальной Собственности от 14.07.1967 г. (редакция 02.10.1979 г.), заключенная в Стокгольме.**
- 7. Конвенция о распространении несущих программы сигналов, передаваемых через спутники от 21.05.1974 г., заключенная в Брюсселе.**

- 8. Евразийская Патентная Конвенция от 09.09.1994 г.,  
заключенная в Москве.**
- 9. Гаагское соглашение по международному  
депонированию промышленных образцов от 06.11.1925  
г. В настоящее время оно носит название "Гаагское  
соглашение о международной регистрации  
промышленных образцов". Переименование произошло  
на Дипломатической конференции в Женеве 02.07.1999 г.  
при подписании Женевского акта Гаагского соглашения о  
международной регистрации промышленных образцов.**
- 10. Международная конвенция об охране интересов  
исполнителей, производителей фонограмм и  
вещательных организаций, от 26.10.1961 г., заключенная  
в Риме.**

РФ не участвует в двух последних.

**Были созданы организации и союзы по охране ИС:**

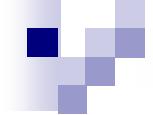
- **Объединенные международные бюро по охране интеллектуальной собственности (БИРПИ)** – международная организация образована в конце 1892 г., предшественница Всемирной организации интеллектуальной собственности (ВОИС);
- **Всемирная Организация Интеллектуальной Собственности (ВОИС)**, основана 14.07.1967 г.;
- **Международный союз по охране промышленной собственности (Парижский союз)**, образованный Парижской конвенцией по охране промышленной собственности от 20.03.1883 г.;
- **Союз по охране прав авторов на их литературные и художественные произведения (Бернский Союз)**, образованный Бернской конвенцией по охране литературных и художественных произведений от 04.12.1887 г.



**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**

Правовая охрана авторских и смежных прав регулируется Разделом VII. Права на результаты интеллектуальной деятельности и средства индивидуализации Части 4 ГК РФ.

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_64629/](https://www.consultant.ru/document/cons_doc_LAW_64629/)

### **Статья 1226 ГК РФ. Интеллектуальные права**

На результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (результаты интеллектуальной деятельности и средства индивидуализации) признаются интеллектуальные права, которые включают исключительное право, являющееся имущественным правом, а в случаях, предусмотренных настоящим Кодексом, также личные неимущественные права и иные права (право следования, право доступа и другие).

# Авторские права регулируются Главой 70. Авторское право Части 4 ГК РФ.

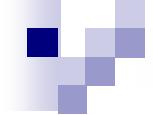
[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_64629/0b318126c43879a845405f1fb1f4342f473a1eda/](https://www.consultant.ru/document/cons_doc_LAW_64629/0b318126c43879a845405f1fb1f4342f473a1eda/)

## Статья 1255 ГК РФ. Авторские права

1. Интеллектуальные права на произведения науки, литературы и искусства являются **авторскими правами**.
2. Автору произведения принадлежат следующие права:
  - 1) исключительное право на произведение;
  - 2) право авторства;
  - 3) право автора на имя;
  - 4) право на неприкосновенность произведения;
  - 5) право на обнародование произведения.
3. В случаях, предусмотренных настоящим Кодексом, автору произведения наряду с правами, указанными в п. 2 настоящей статьи, принадлежат другие права, в том числе право на вознаграждение за служебное произведение, право на отзыв, право следования, право доступа к произведениям изобразительного искусства.

**Авторское право** распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой либо объективной форме:

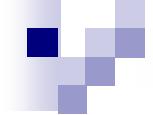
- **письменной**;
- **устной** (выступление, исполнение и т.д.);
- **звуко- или видеозаписи**;
- **изображения** (рисунок, чертеж, теле-, фотокадр и т.д.);
- **объемно-пространственной** (скульптура, макет и т.д.);
- **в других формах**.



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 ст. 1262 Гражданского Кодекса).**

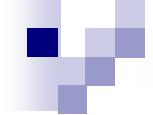
Обладатель исключительных авторских прав для оповещения о своих правах вправе использовать **знак охраны авторского права**, который помещается на каждом экземпляре произведения и состоит из трех элементов:

- латинской буквы “С” в окружности ©;
- имени (наименования) обладателя исключительных прав;
- года первого опубликования произведения.

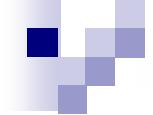
УДК 378.046:004.1(075.8)  
ББК 70+74.58+32.81

ISBN 978-5-4365-9368-5

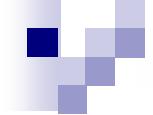
© Некрасов А.В., 2022  
© ООО «РУСАЙНС», 2022



**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** (п. 1 ст. 1281 ГК РФ).

## Историческая справка

В сфере авторского права до 70-х годов прошлого века в СССР 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**.

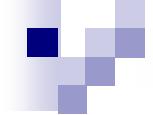
В 2004 г. были приняты поправки к Закону РФ “Об авторском праве и смежных правах” где действие авторского права установлено с учетом действующих международных норм в течении всей жизни автора и **70 лет** после его смерти.



Поправки, вступившие в силу с 1 сентября 2006 г., означают, что размещенные в сети, например, тексты книг или музыкальные файлы в формате тр3 охраняются авторским правом так же, как обычные книги или компакт-диски.

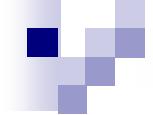
Они подпадают под действие ст. 146 Уголовного кодекса РФ ("Нарушение авторских и смежных прав"), предусматривающей наказание для пиратов в виде **лишения свободы на срок до шести лет.**

**Владельцы тр3-сайтов** теперь должны подписать лицензионные соглашения со всеми поставщиками музыки.



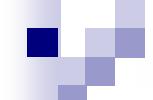
**Истечение срока действия авторского права на произведения означает их переход в общественное достояние (ст. 1282 ГК РФ).**

**Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно.**



**Знак охраны смежных прав – латинская буква “Р” в окружности (Р), 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, переделывать, продавать и воспроизводить без разрешения их правообладателей.**

Смежные права регулируются Главой 71. Права, смежные с авторскими Части 4 ГК РФ.

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_64629/78ed072f32b5cd926608d72a66e72cf885ec99dc/](https://www.consultant.ru/document/cons_doc_LAW_64629/78ed072f32b5cd926608d72a66e72cf885ec99dc/)

## **Статья 1303 ГК РФ. Основные положения**

1. Интеллектуальные права на результаты исполнительской деятельности (исполнения), на фонограммы, на сообщение в эфир или по кабелю радио- и телепередач (вещание организаций эфирного и кабельного вещания), на содержание баз данных, а также на произведения науки, литературы и искусства, впервые обнародованные после их перехода в общественное достояние, являются **смежными с авторскими правами (смежными правами)**.
2. К смежным правам относится исключительное право, а в случаях, предусмотренных настоящим Кодексом, относятся также личные неимущественные права.
3. Смежные права осуществляются с соблюдением авторских прав на произведения науки, литературы и искусства, использованные при создании объектов смежных прав. Смежные права признаются и действуют независимо от наличия и действия авторских прав на такие произведения.

## Статья 1304 ГК РФ. Объекты смежных прав

1. Объектами смежных прав являются:

- 1) результаты исполнительской деятельности (исполнения), к которым относятся исполнения артистов-исполнителей и дирижеров, если эти исполнения выражаются в форме, допускающей их воспроизведение и распространение с помощью технических средств, постановки режиссеров-постановщиков спектаклей, если эти постановки выражаются в форме, позволяющей осуществить их повторное публичное исполнение при сохранении узнаваемости конкретной постановки зрителями, а также в форме, допускающей воспроизведение и распространение с помощью технических средств;
- 2) фонограммы, то есть любые исключительно звуковые записи исполнений или иных звуков либо их отображений, за исключением звуковой записи, включенной в аудиовизуальное произведение;
- 3) сообщения передач организаций эфирного или кабельного вещания, в том числе передач, созданных самой организацией эфирного или кабельного вещания либо по ее заказу за счет ее средств другой организацией;
- 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.
  2. Для возникновения, осуществления и защиты смежных прав не требуется регистрация их объекта или соблюдение каких-либо иных формальностей.
  3. Предоставление на территории Российской Федерации охраны объектам смежных прав в соответствии с международными договорами Российской Федерации осуществляется в отношении исполнений, фонограмм, сообщений передач организаций эфирного или кабельного вещания, не перешедших в общественное достояние в стране их происхождения вследствие истечения установленного в такой стране срока действия исключительного права на эти объекты и не перешедших в общественное достояние в Российской Федерации вследствие истечения предусмотренного настоящим Кодексом срока действия исключительного права.

## **Статья 1245 ГК РФ. Вознаграждение за свободное воспроизведение фонограмм и аудиовизуальных произведений в личных целях**

1. Авторам, исполнителям, изготовителям фонограмм и аудиовизуальных произведений принадлежит право на вознаграждение за свободное воспроизведение фонограмм и аудиовизуальных произведений исключительно в личных целях. Такое вознаграждение имеет компенсационный характер и выплачивается правообладателям за счет средств, которые подлежат уплате изготовителями и импортерами оборудования и материальных носителей, используемых для такого воспроизведения.

Перечень оборудования и материальных носителей, а также размер и порядок сбора соответствующих средств утверждаются Правительством Российской Федерации.

2. Сбор средств для выплаты вознаграждения за свободное воспроизведение фонограмм и аудиовизуальных произведений в личных целях осуществляется аккредитованной организацией (статья 1244).

3. Вознаграждение за свободное воспроизведение фонограмм и аудиовизуальных произведений в личных целях распределяется между правообладателями в следующей пропорции: **40% - авторам, 30% - исполнителям, 30% - изготовителям фонограмм или аудиовизуальных произведений.**
- Распределение вознаграждения между конкретными авторами, исполнителями, изготовителями фонограмм или аудиовизуальных произведений осуществляется пропорционально фактическому использованию соответствующих фонограмм или аудиовизуальных произведений. Порядок распределения вознаграждения и его выплаты устанавливается Правительством Российской Федерации.
4. Средства для выплаты вознаграждения за свободное воспроизведение фонограмм и аудиовизуальных произведений в личных целях не взимаются с изготовителей того оборудования и тех материальных носителей, которые являются предметом экспорта, а также с изготовителей и импортеров профессионального оборудования, не предназначенного для использования в домашних условиях.

## **Статья 1273 ГК РФ. Свободное воспроизведение произведения в личных целях**

1. Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином при необходимости и исключительно в личных целях правомерно обнародованного произведения, за исключением:
- 1) воспроизведения произведений архитектуры в форме зданий и аналогичных сооружений;
  - 2) воспроизведения баз данных или их существенных частей, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса;
  - 3) воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса;
  - 4) репродуцирования книг (полностью) и нотных текстов (статья 1275), то есть их факсимильного воспроизведения с помощью любых технических средств, осуществляемого не в целях издания;

- 
- 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.
2. В случае, когда воспроизведение фонограмм и аудиовизуальных произведений осуществляется исключительно в личных целях, авторы, исполнители, изготовители фонограмм и аудиовизуальных произведений имеют право на вознаграждение, предусмотренное статьей 1245 настоящего Кодекса.



## Статья 1326 ГК РФ. Использование фонограммы, опубликованной в коммерческих целях

1. Публичное исполнение фонограммы, опубликованной в коммерческих целях, а также ее сообщение в эфир или по кабелю допускается без разрешения обладателя исключительного права на фонограмму и обладателя исключительного права на зафиксированное в этой фонограмме исполнение, но с выплатой им вознаграждения.
2. Сбор с пользователей вознаграждения, предусмотренного пунктом 1 настоящей статьи, и распределение этого вознаграждения осуществляются организациями по управлению правами на коллективной основе, имеющими государственную аккредитацию на осуществление соответствующих видов деятельности (статья 1244).

3. Вознаграждение, предусмотренное пунктом 1 настоящей статьи, распределяется между правообладателями в пропорции, составляющей **50% - исполнителям, 50% - изготовителям фонограмм**. Распределение вознаграждения между конкретными исполнителями, изготовителями фонограмм осуществляется пропорционально фактическому использованию соответствующих фонограмм. Правительство Российской Федерации вправе устанавливать ставки вознаграждения, а также порядок сбора, распределения и выплаты вознаграждения.
4. Пользователи фонограмм должны представлять в организацию по управлению правами на коллективной основе отчеты об использовании фонограмм, а также иные сведения и документы, необходимые для сбора и распределения вознаграждения.

## Статья 1337 ГК РФ. Публикатор

1. Публикатором признается гражданин, который правомерно обнародовал или организовал обнародование произведения науки, литературы или искусства, ранее не обнародованного и перешедшего в общественное достояние (статья 1282) либо находящегося в общественном достоянии в силу того, что оно не охранялось авторским правом.
2. Права публикатора распространяются на произведения, которые независимо от времени их создания могли быть признаны объектами авторского права в соответствии с правилами статьи 1259 настоящего Кодекса.
3. Положения, предусмотренные настоящим параграфом, не распространяются на произведения, находящиеся в государственных и муниципальных архивах.

## Статья 1338 ГК РФ. Права публикатора

1. Публикатору принадлежат:

1) исключительное право публикатора на обнародованное им произведение (пункт 1 статьи 1339);  
2) право на указание своего имени на экземплярах обнародованного им произведения и в иных случаях его использования, в том числе при переводе или другой переработке произведения.

2. При обнародовании произведения публикатор обязан соблюдать условия, предусмотренные пунктом 3 статьи 1268 настоящего Кодекса.

3. Публикатор в течение срока действия исключительного права публикатора на произведение обладает правомочиями, указанными в абзаце втором пункта 1 статьи 1266 настоящего Кодекса. Такими же правомочиями обладает лицо, к которому перешло исключительное право публикатора на произведение.

## **Статья 1339 ГК РФ. Исключительное право публикатора на произведение**

1. Публикатору произведения принадлежит исключительное право использовать произведение в соответствии со статьей 1229 настоящего Кодекса (исключительное право публикатора на произведение) способами, предусмотренными подпунктами 1 - 8.1 и 11 пункта 2 статьи 1270 настоящего Кодекса. Публикатор произведения может распоряжаться указанным исключительным правом.
2. Исключительное право публикатора на произведение признается и в том случае, когда произведение было обнародовано публикатором в переводе или в виде иной переработки. Исключительное право публикатора на произведение признается и действует независимо от наличия и действия авторского права публикатора или других лиц на перевод или иную переработку произведения.

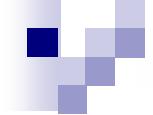


## Статья 1340 ГК РФ. Срок действия исключительного права публикатора на произведение

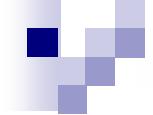
- Исключительное право публикатора** на произведение возникает в момент обнародования этого произведения и **действует в течение двадцати пяти лет**, считая с 1 января года, следующего за годом его обнародования.
- После прекращения действия исключительного права публикатора произведение может свободно использоваться любым лицом без чьего-либо согласия или разрешения и без выплаты вознаграждения.

## **Статья 1341 ГК РФ. Действие исключительного права публикатора на произведение на территории Российской Федерации**

1. Исключительное право публикатора распространяется на произведение:
  - 1) обнародованное на территории Российской Федерации, независимо от гражданства публикатора;
  - 2) обнародованное за пределами территории Российской Федерации гражданином Российской Федерации;
  - 3) обнародованное за пределами территории Российской Федерации иностранным гражданином или лицом без гражданства, при условии, что законодательством иностранного государства, в котором обнародовано произведение, предоставляемое на его территории охрана исключительному праву публикатора, являющегося гражданином Российской Федерации;



- 4) в иных случаях, предусмотренных международными договорами Российской Федерации.
2. В случае, указанном в подпункте 3 пункта 1 настоящей статьи, срок действия исключительного права публикатора на произведение на территории Российской Федерации не может превышать срок действия исключительного права публикатора на произведение, установленный в государстве, на территории которого имел место юридический факт, послуживший основанием для приобретения такого исключительного права.



**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**.
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, - **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 до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок **до двух лет**, либо лишением свободы на тот же срок.

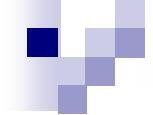
3. Деяния, предусмотренные частью второй настоящей статьи, если они совершены:

б) группой лиц по предварительному сговору или организованной группой;

в) в особо крупном размере;

г) лицом с использованием своего служебного положения, - **наказывается принудительными работами на срок до пяти лет либо 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 или без такового.**

Примечание. Деяния, предусмотренные настоящей статьей, признаются совершенными в крупном размере, если стоимость экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав превышают сто тысяч рублей, а в особо крупном размере - один миллион рублей.



## 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.**
- 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**

**Доценты кафедры БИТ**

**Струков Владимир Ильич  
Некрасов Алексей Валентинович**



## Вопросы к разделу 10.1

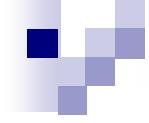
- 1. Назовите правовые формы охраны интеллектуальной собственности.**
- 2. Что понимается под исключительными правами на объекты интеллектуальной собственности?**
- 3. Международные конвенции и соглашения, связанные с охраной интеллектуальной собственности.**
- 4. Правовая охрана авторских и смежных 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 1991 г., когда были приняты **Основы гражданского законодательства СССР и союзных республик.**

**Закон “О правовой охране программ для ЭВМ и баз данных” от 23.09.1992 г. № 3523** регулировал до 2008 г. 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.**



## Статья 1261 ГК РФ. Программы для ЭВМ

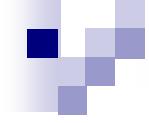
Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. Программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.



## Статья 1262 ГК РФ. Государственная регистрация программ для ЭВМ и баз данных

1. 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. Лицо, подавшее заявку на государственную регистрацию (заявитель), несет ответственность за разглашение сведений о программах для ЭВМ и базах данных, в которых содержатся сведения, составляющие государственную тайну, в соответствии с законодательством Российской Федерации.



2. Заявка на государственную регистрацию программы для ЭВМ или базы данных (заявка на регистрацию) должна относиться к одной программе для ЭВМ или к одной базе данных.

Заявка на регистрацию должна содержать:

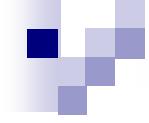
- заявление о государственной регистрации программы для ЭВМ или базы данных с указанием правообладателя, а также автора, если он не отказался быть упомянутым в качестве такового, и места жительства или места нахождения каждого из них;
- депонируемые материалы, идентифицирующие программу для ЭВМ или базу данных, включая реферат.

Правила оформления заявки на регистрацию устанавливает федеральный орган исполнительной власти, осуществляющий нормативно-правовое регулирование в сфере интеллектуальной собственности.

3. На основании заявки на регистрацию федеральный орган исполнительной власти по интеллектуальной собственности проверяет наличие необходимых документов и материалов, их соответствие требованиям, предусмотренным пунктом 2 настоящей статьи. При положительном результате проверки указанный федеральный орган вносит программу для ЭВМ или базу данных соответственно в Реестр программ для ЭВМ и в Реестр баз данных, выдает заявителю свидетельство о государственной регистрации в форме электронного документа и по желанию заявителя на бумажном носителе, публикует сведения о зарегистрированных программах для ЭВМ или базе данных в официальном бюллетене этого органа.

По запросу указанного федерального органа либо по собственной инициативе автор или иной правообладатель вправе до момента государственной регистрации программы для ЭВМ или базы данных дополнять, уточнять и исправлять документы и материалы, содержащиеся в заявке на регистрацию.

- 
4. Порядок государственной регистрации программ для ЭВМ и баз данных, формы свидетельств о государственной регистрации, перечень указываемых в них сведений и перечень сведений, публикуемых в официальном бюллетене федерального органа исполнительной власти по интеллектуальной собственности, устанавливаются федеральным органом исполнительной власти, осуществляющим нормативно-правовое регулирование в сфере интеллектуальной собственности.
  5. Переход исключительного права на зарегистрированные программу для ЭВМ или базу данных к другому лицу по договору или без договора и залог исключительного права на зарегистрированные программу для ЭВМ или базу данных подлежат государственной регистрации в федеральном органе исполнительной власти по интеллектуальной собственности.



5.1. По заявлению правообладателя федеральный орган исполнительной власти по интеллектуальной собственности вносит изменения, относящиеся к сведениям о правообладателе и (или) об авторе программы для ЭВМ или базы данных, в том числе к наименованию или имени правообладателя, его месту нахождения или месту жительства, имени автора, адресу для переписки, а также изменения, связанные с исправлением очевидных и технических ошибок, в Реестр программ для ЭВМ или Реестр баз данных и свидетельство о государственной регистрации.

Федеральный орган исполнительной власти по интеллектуальной собственности может вносить изменения в Реестр программ для ЭВМ или Реестр баз данных для исправления очевидных и технических ошибок по собственной инициативе или по просьбе любого лица, предварительно уведомив об этом правообладателя.



Федеральный орган исполнительной власти по интеллектуальной собственности публикует в официальном бюллетене сведения об изменениях записей в Реестре программ для ЭВМ или Реестре баз данных.

6. Сведения, внесенные в Реестр программ для ЭВМ или в Реестр баз данных, считаются достоверными, поскольку не доказано иное. Ответственность за достоверность предоставленных для государственной регистрации сведений несет заявитель.

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.



## Статья 1280 ГК РФ. Право пользователя программы для ЭВМ и базы данных

1. Лицо, lawfully owning an exemplar of a program for a computer or a database exemplar (user), has the right without the author's or other right holder's permission and without payment of additional remuneration:
  - 1) to perform actions necessary for the functioning of a program for a computer or a database (including during its use in accordance with their purpose), including recording and storage in the memory of a computer (one computer or one user of a network), entry into a program for a computer or a database, making changes to the data in it exclusively for the purposes of its functioning on technical means of the user, correction of obvious errors, if otherwise not provided for by the contract with the right holder;



- 2) изготавливать копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные в подпункте 1 настоящего пункта, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.
2. Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления действий, предусмотренных подпунктом 1 пункта 1 настоящей статьи.

3. Лицо, lawfully владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

- 1) информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;
- 2) указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;



- 3) информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.
4. Применение положений, предусмотренных настоящей статьей, не должно противоречить обычному использованию программы для ЭВМ или базы данных и не должно ущемлять необоснованным образом законные интересы автора или иного правообладателя.

## **Статья 1335 ГК РФ. Срок действия исключительного права изготовителя базы данных**

- 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.
- Сроки, предусмотренные пунктом 1 настоящей статьи, **возобновляются при каждом обновлении базы данных**.

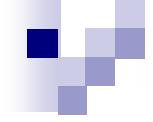
## ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ АВТОРСКИХ ПРАВ

### Статья 1299 ГК РФ. 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 **устранить 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** положений, предусмотренных  
пунктом 2 настоящей статьи, автор или иной  
 правообладатель вправе **требовать** по своему выбору от  
нарушителя **возмещения убытков или выплаты**  
**компенсации** в соответствии со статьей 1301 настоящего  
Кодекса.



4. В случае, если пунктами 1-3 статьи 1274 и статьей 1278 настоящего Кодекса разрешено использование произведения без согласия автора или иного правообладателя и такое использование невозможно осуществить в силу наличия технических средств защиты авторских прав, лицо, правомерно претендующее на осуществление такого использования, может требовать от автора или иного правообладателя снять ограничения использования произведения, установленные путем применения технических средств защиты авторских прав, либо предоставить возможность такого использования по выбору правообладателя при условии, что это технически возможно и не требует существенных затрат.

## ОХРАНА ТОПОЛОГИИ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

### **Статья 1448 ГК РФ. Топология интегральной микросхемы**

1. Топологией интегральной микросхемы является зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы (ИМС) и связей между ними. При этом интегральной микросхемой является микроэлектронное изделие окончательной или промежуточной формы, которое предназначено для выполнения функций электронной схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено такое изделие.

2. Правовая охрана, предоставляемая настоящим Кодексом, распространяется только на оригинальную топологию интегральной микросхемы, созданную в результате творческой деятельности автора и неизвестную автору и (или) специалистам в области разработки топологий интегральных микросхем на дату ее создания. Топология интегральной микросхемы признается оригинальной, пока не доказано обратное.

Топологии интегральной микросхемы, состоящей из элементов, которые известны специалистам в области разработки топологий интегральных микросхем на дату ее создания, предоставляется правовая охрана, если пространственно-геометрическое расположение совокупности таких элементов и связей между ними в целом отвечает требованию оригинальности.

3. Правовая охрана, предоставляемая настоящим Кодексом, не распространяется на идеи, способы, системы, технологию или закодированную информацию, которые могут быть воплощены в топологии интегральной микросхемы.

## **Статья 1449 ГК РФ. Права на топологию интегральной микросхемы**

1. Автору топологии интегральной микросхемы, отвечающей условиям предоставления правовой охраны, предусмотренным настоящим Кодексом (топологии), принадлежат следующие **интеллектуальные права**:
  - 1) исключительное право;
  - 2) право авторства.
2. В случаях, предусмотренных настоящим Кодексом, автору топологии интегральной микросхемы принадлежат также другие права, в том числе право на вознаграждение за служебную топологию.



## Статья 1450 ГК РФ. Автор топологии интегральной микросхемы

Автором топологии интегральной микросхемы признается гражданин, творческим трудом которого создана такая топология. Лицо, указанное в качестве автора в заявке на выдачу свидетельства о государственной регистрации топологии интегральной микросхемы, считается автором этой топологии, если не доказано иное.



## Статья 1451 ГК РФ. Соавторы топологии интегральной микросхемы

1. Граждане, создавшие топологию интегральной микросхемы совместным творческим трудом, признаются соавторами.
2. Каждый из соавторов вправе использовать топологию по своему усмотрению, если соглашением между ними не предусмотрено иное.
3. К отношениям соавторов, связанным с распределением доходов от использования топологии и с распоряжением исключительным правом на топологию, соответственно применяются правила пункта 3 статьи 1229 настоящего Кодекса.

Распоряжение правом на получение свидетельства о государственной регистрации топологии интегральной микросхемы осуществляется соавторами совместно.

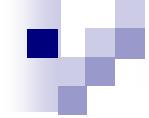


## Статья 1452 ГК РФ. Государственная регистрация топологии интегральной микросхемы

1. Правообладатель в течение срока действия исключительного права на топологию интегральной микросхемы (статья 1457) может по своему желанию зарегистрировать топологию в федеральном органе исполнительной власти по интеллектуальной собственности.

Топология, содержащая сведения, составляющие государственную тайну, государственной регистрации не подлежит. Лицо, подавшее заявку на государственную регистрацию топологии (заявитель), несет ответственность за разглашение сведений о топологии, содержащей государственную тайну, в соответствии с законодательством Российской Федерации.

2. Если до подачи заявки на государственную регистрацию топологии (заявка на регистрацию) имело место использование топологии, заявка может быть подана в срок, не превышающий двух лет со дня первого использования топологии.



3. 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;
4. Правила оформления заявки на регистрацию устанавливаются федеральным органом исполнительной власти, осуществляющим нормативно-правовое регулирование в сфере интеллектуальной собственности.

5. На основании заявки на регистрацию федеральный орган исполнительной власти по интеллектуальной собственности проверяет наличие необходимых документов и их соответствие требованиям пункта 3 настоящей статьи. При положительном результате проверки указанный федеральный орган вносит топологию в Реестр топологий интегральных микросхем, выдает заявителю свидетельство о государственной регистрации топологии интегральной микросхемы в форме электронного документа и по желанию заявителя на бумажном носителе и публикует сведения о зарегистрированной топологии в официальном бюллетене.

По запросу указанного федерального органа исполнительной власти либо по собственной инициативе автор или иной правообладатель вправе до момента государственной регистрации дополнять, уточнять и исправлять материалы заявки на регистрацию.

6. Порядок государственной регистрации топологий, формы свидетельств о государственной регистрации, перечень указываемых в свидетельствах сведений и перечень сведений, публикуемых федеральным органом исполнительной власти по интеллектуальной собственности в официальном бюллетене, устанавливаются федеральным органом исполнительной власти, осуществляющим нормативно-правовое регулирование в сфере интеллектуальной собственности. По запросу указанного федерального органа исполнительной власти либо по собственной инициативе автор или иной правообладатель вправе до момента государственной регистрации дополнять, уточнять и исправлять материалы заявки на регистрацию.

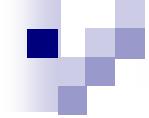
7. По заявлению правообладателя федеральный орган исполнительной власти по интеллектуальной собственности вносит изменения, относящиеся к сведениям о правообладателе и (или) об авторе топологии, в том числе к наименованию или имени правообладателя, его месту нахождения или месту жительства, имени автора топологии, адресу для переписки, а также изменения для исправления очевидных и технических ошибок в Реестр топологий интегральных микросхем и свидетельство о государственной регистрации топологии.

Федеральный орган исполнительной власти по интеллектуальной собственности публикует в официальном бюллетене сведения о любых изменениях записей, внесенных в Реестр топологий интегральных микросхем.

8. Сведения, внесенные в Реестр топологий интегральных микросхем, считаются достоверными, если не доказано иное. Ответственность за достоверность представленных для регистрации сведений несет заявитель.

## **Статья 1454 ГК РФ. Исключительное право на топологию**

1. Правообладателю принадлежит **исключительное право использования топологии** в соответствии со статьей 1229 настоящего Кодекса любым не противоречащим закону способом (исключительное право на топологию), в том числе способами, указанными в пункте 2 настоящей статьи. Правообладатель может распоряжаться исключительным правом на топологию.
2. **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, включающего в себя такую интегральную микросхему.**
3. За лицом, независимо создавшим топологию, идентичную другой топологии, признается самостоятельное исключительное право на эту топологию.

## **Статья 1455 ГК РФ. Знак охраны топологии интегральной микросхемы**

**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.**

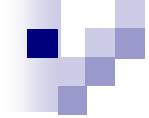
## Статья 1461 ГК РФ. Служебная топология

1. Топология, созданная работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, признается **служебной топологией**.
2. Право авторства на служебную топологию принадлежит работнику.
3. Исключительное право на служебную топологию принадлежит работодателю, если трудовым или гражданско-правовым договором между ним и работником не предусмотрено иное.
4. Если исключительное право на топологию принадлежит работодателю или передано им третьему лицу, работник имеет право на получение от работодателя вознаграждения. Размер вознаграждения, условия и порядок его выплаты определяются договором между работником и работодателем, а в случае спора – судом.

Право на вознаграждение за служебную топологию неотчуждаемо, но переходит к наследникам автора на оставшийся срок действия исключительного права.

В случае, если исключительное право на топологию принадлежит автору, работодатель имеет право использования такой топологии на условиях простой (неисключительной) лицензии с выплатой правообладателю вознаграждения.

5. Топология, созданная работником с использованием денежных, технических или иных материальных средств работодателя, но не в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя, не является служебной. Исключительное право на такую топологию принадлежит работнику. В этом случае работодатель имеет право по своему выбору потребовать предоставления безвозмездной простой (неисключительной) лицензии на использование созданной топологии для собственных нужд на весь срок действия исключительного права на топологию или возмещения расходов, понесенных им в связи с созданием такой топологии.



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**.

## ОХРАНА ПАТЕНТНЫХ ПРАВ

**Изобретение** – 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), в том числе к применению продукта или способа по определенному назначению. Изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо (ст. 1350 ГК РФ).

**Полезная модель** – техническое решение, относящееся к устройству. Полезной модели предоставляется правовая охрана, если она является новой и промышленно применимой (ст. 1351 ГК РФ).

**Промышленный образец** – решение внешнего вида изделия промышленного или кустарно-ремесленного производства. Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным. (ст. 1352 ГК РФ).

Патентные права регулируются Главой 72. Патентное право Части 4 ГК РФ.

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_64629/630108e4684aa4aacf1ea63101d1ab76f26eca7/](https://www.consultant.ru/document/cons_doc_LAW_64629/630108e4684aa4aacf1ea63101d1ab76f26eca7/)

## **Статья 1345 ГК РФ. Патентные права**

1. Интеллектуальные права на изобретения, полезные модели и промышленные образцы являются **патентными правами**.
2. Автору изобретения, полезной модели или промышленного образца принадлежат следующие права:
  - 1) исключительное право;
  - 2) право авторства.
3. В случаях, предусмотренных настоящим Кодексом, автору изобретения, полезной модели или промышленного образца принадлежат также другие права, в том числе право на получение патента, право на вознаграждение за служебное изобретение, полезную модель или промышленный образец.

## **Статья 1346 ГК РФ. Действие исключительных прав на изобретения, полезные модели и промышленные образцы на территории Российской Федерации**

На территории Российской Федерации признаются исключительные права на изобретения, полезные модели и промышленные образцы, удостоверенные патентами, выданными федеральным органом исполнительной власти по интеллектуальной собственности, а также в других случаях, предусмотренных международными договорами РФ.

## **Статья 1347 ГК РФ. Автор изобретения, полезной модели или промышленного образца**

Автором изобретения, полезной модели или промышленного образца признается гражданин, творческим трудом которого создан соответствующий результат интеллектуальной деятельности. Лицо, указанное в качестве автора в заявке на выдачу патента на изобретение, полезную модель или промышленный образец, считается автором изобретения, полезной модели или промышленного образца, если не доказано иное.

## **Статья 1348 ГК РФ. Соавторы изобретения, полезной модели или промышленного образца**

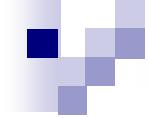
1. Граждане, создавшие изобретение, полезную модель или промышленный образец совместным творческим трудом, признаются соавторами.
2. Каждый из соавторов вправе использовать изобретение, полезную модель или промышленный образец по своему усмотрению, если соглашением между ними не предусмотрено иное.
3. К отношениям соавторов, связанным с распределением доходов от использования изобретения, полезной модели или промышленного образца и с распоряжением исключительным правом на изобретение, полезную модель или промышленный образец, соответственно применяются правила пункта 3 статьи 1229 настоящего Кодекса.

Распоряжение правом на получение патента на изобретение, полезную модель или промышленный образец осуществляется авторами совместно.

4. Каждый из соавторов вправе самостоятельно принимать меры по защите своих прав на изобретение, полезную модель или промышленный образец.

## **Статья 1349 УК РФ. Объекты патентных прав**

- 1. Объектами патентных прав являются результаты интеллектуальной деятельности в научно-технической сфере, отвечающие установленным настоящим Кодексом требованиям к изобретениям и полезным моделям, и результаты интеллектуальной деятельности в сфере дизайна, отвечающие установленным настоящим Кодексом требованиям к промышленным образцам.**
- 2. На изобретения, содержащие сведения, составляющие государственную тайну (секретные изобретения), положения настоящего Кодекса распространяются, если иное не предусмотрено специальными правилами статей 1401 - 1405 настоящего Кодекса и изданными в соответствии с ними иными правовыми актами.**



3. Полезным моделям и промышленным образцам, содержащим сведения, составляющие государственную тайну, правовая охрана в соответствии с настоящим Кодексом не предоставляется.
4. Не могут быть объектами патентных прав:
  - 1) способы клонирования человека и его клон;
  - 2) способы модификации генетической целостности клеток зародышевой линии человека;
  - 3) использование человеческих эмбрионов в промышленных и коммерческих целях;
  - 4) результаты интеллектуальной деятельности, указанные в пункте 1 настоящей статьи, если они противоречат общественным интересам, принципам гуманности и морали.

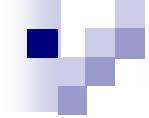
## Статья 1350 ГК РФ. Условия патентоспособности изобретения

1. 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), в том числе к применению продукта или способа по определенному назначению.

Изобретению предоставляется правовая охрана, если оно является новым, имеет изобретательский уровень и промышленно применимо.

2. 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.



Уровень техники для изобретения включает любые сведения, ставшие общедоступными в мире до даты приоритета изобретения.

При установлении новизны изобретения в уровень техники также включаются при условии их более раннего приоритета все поданные в Российской Федерации другими лицами заявки на выдачу патентов на изобретения, полезные модели и промышленные образцы, с документами которых вправе ознакомиться любое лицо в соответствии с пунктами 2 и 4 статьи 1385 или пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации изобретения, полезные модели и промышленные образцы.

3. Раскрытие информации, относящейся к изобретению, автором изобретения, заявителем либо любым получившим от них прямо или косвенно эту информацию лицом (в том числе в результате экспонирования изобретения на выставке), вследствие чего сведения о сущности изобретения стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности изобретения, при условии, что заявка на выдачу патента на изобретение подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности изобретения, имели место, лежит на заявителе.
4. Изобретение является промышленно применимым, если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

5. Не являются изобретениями, в частности:

- 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.

В соответствии с настоящим пунктом исключается возможность отнесения этих объектов к изобретениям только в случае, когда заявка на выдачу патента на изобретение касается этих объектов как таковых.

6. Не предоставляется правовая охрана в качестве изобретения:

- 1) сортам растений, породам животных и биологическим способам их получения, то есть способам, полностью состоящим из скрещивания и отбора, за исключением микробиологических способов и полученных такими способами продуктов;
- 2) топологиям интегральных микросхем.

## Статья 1351 ГК РФ. Условия патентоспособности полезной модели

1. В качестве полезной модели охраняется техническое решение, относящееся к устройству.

Полезной модели предоставляется правовая охрана, если она является новой и промышленно применимой.

2. Полезная модель является новой, если совокупность ее существенных признаков не известна из уровня техники.

Уровень техники в отношении полезной модели включает любые сведения, ставшие общедоступными в мире до даты приоритета полезной модели. В уровень техники также включаются (при условии более раннего приоритета) все заявки на выдачу патента на изобретение, полезную модель или промышленный образец, которые поданы в Российской Федерации другими лицами и с документами которых вправе ознакомиться любое лицо в соответствии с пунктами 2 и 4 статьи 1385 или пунктом 2 статьи 1394 настоящего Кодекса, и запатентованные в Российской Федерации изобретения и полезные модели.

3. Раскрытие информации, относящейся к полезной модели, автором полезной модели, заявителем либо любым получившим от них прямо или косвенно эту информацию лицом (в том числе в результате экспонирования полезной модели на выставке), вследствие чего сведения о сущности полезной модели стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности полезной модели, при условии, что заявка на выдачу патента на полезную модель подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение шести месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности полезной модели, имели место, лежит на заявителе.
4. Полезная модель является промышленно применимой, если она может быть использована в промышленности, сельском хозяйстве, здравоохранении, других отраслях экономики или в социальной сфере.

5. Не являются полезными моделями, в частности, объекты, указанные в пункте 5 статьи 1350 настоящего Кодекса. В соответствии с настоящим пунктом исключается возможность отнесения указанных объектов к полезным моделям только в случае, если заявка на выдачу патента на полезную модель касается указанных объектов как таковых.
6. Не предоставляется правовая охрана в качестве полезной модели объектам, указанным в пункте 6 статьи 1350 настоящего Кодекса.

## **Статья 1352 ГК РФ. Условия патентоспособности промышленного образца**

1. В качестве промышленного образца охраняется решение внешнего вида изделия промышленного или кустарно-ремесленного производства.

Промышленному образцу предоставляется правовая охрана, если по своим существенным признакам он является новым и оригинальным.



К существенным признакам промышленного образца относятся признаки, определяющие эстетические особенности внешнего вида изделия, в частности форма, конфигурация, орнамент, сочетание цветов, линий, контуры изделия, текстура или фактура материала изделия.

Признаки, обусловленные исключительно технической функцией изделия, не являются охраняемыми признаками промышленного образца.

2. Промышленный образец является новым, если совокупность его существенных признаков, нашедших отражение на изображениях внешнего вида изделия, не известна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца.

3. Промышленный образец является оригинальным, если его существенные признаки обусловлены творческим характером особенностей изделия, в частности если из сведений, ставших общедоступными в мире до даты приоритета промышленного образца, неизвестно решение внешнего вида изделия сходного назначения, производящее на информированного потребителя такое же общее впечатление, какое производит промышленный образец, нашедший отражение на изображениях внешнего вида изделия.
4. При установлении новизны и оригинальности промышленного образца также учитываются (при условии более раннего приоритета) все заявки на изобретения, полезные модели, промышленные образцы и заявки на государственную регистрацию товарных знаков, знаков обслуживания, которые поданы в Российской Федерации другими лицами и с документами которых в соответствии с пунктами 2 и 4 статьи 1385, пунктом 2 статьи 1394, пунктом 1 статьи 1493 настоящего Кодекса вправе ознакомиться любое лицо.

Раскрытие информации, относящейся к промышленному образцу, автором промышленного образца, заявителем либо любым получившим от них прямо или косвенно эту информацию лицом (в том числе в результате экспонирования промышленного образца на выставке), вследствие чего сведения о сущности промышленного образца стали общедоступными, не является обстоятельством, препятствующим признанию патентоспособности промышленного образца, при условии, что заявка на выдачу патента на промышленный образец подана в федеральный орган исполнительной власти по интеллектуальной собственности в течение двенадцати месяцев со дня раскрытия информации. Бремя доказывания того, что обстоятельства, в силу которых раскрытие информации не препятствует признанию патентоспособности промышленного образца, имели место, лежит на заявителе.



## 5. Не предоставляется правовая охрана в качестве промышленного образца:

- 1) решениям, все признаки которых обусловлены исключительно технической функцией изделия;
- 2) решениям, способным ввести в заблуждение потребителя изделия, в том числе в отношении производителя изделия, или места производства изделия, или товара, для которого изделие служит тарой, упаковкой, этикеткой, в частности решениям, идентичным объектам, указанным в пунктах 4 - 9 статьи 1483 настоящего Кодекса, либо производящим такое же общее впечатление, либо включающим указанные объекты, если права на указанные объекты возникли ранее даты приоритета промышленного образца, за исключением случаев, если правовая охрана промышленного образца испрашивается лицом, имеющим исключительное право на такой объект.

Предоставление правовой охраны промышленным образцам, идентичным объектам, указанным в пункте 4, подпунктах 1, 2 пункта 9 статьи 1483 настоящего Кодекса, либо производящим такое же общее впечатление, либо включающим указанные объекты, допускается с согласия собственников или уполномоченных собственниками лиц либо обладателей прав на указанные объекты.

## **Статья 1353 ГК РФ. Государственная регистрация изобретений, полезных моделей и промышленных образцов**

1. В качестве промышленного образца охраняется решение внешнего вида изделия промышленного или кустарно-ремесленного производства.

**Исключительное право** на изобретение, полезную модель или промышленный образец **признается и охраняется при условии государственной регистрации соответствующих изобретения, полезной модели или промышленного образца**, на основании которой федеральный орган исполнительной власти по интеллектуальной собственности выдает патент на изобретение, полезную модель или промышленный образец.

## Статья 1354 ГК РФ. Патент на изобретение, полезную модель или промышленный образец

1. Патент на изобретение, полезную модель или промышленный образец удостоверяет приоритет изобретения, полезной модели или промышленного образца, авторство и исключительное право на изобретение, полезную модель или промышленный образец.
2. Охрана интеллектуальных прав на изобретение или полезную модель предоставляется на основании патента в объеме, определяемом содержащейся в патенте формулой изобретения или соответственно полезной модели. Для толкования формулы изобретения и формулы полезной модели могут использоваться описание и чертежи, а также трехмерные модели изобретения и полезной модели в электронной форме (пункт 2 статьи 1375 и пункт 2 статьи 1376).
3. Охрана интеллектуальных прав на промышленный образец предоставляется на основании патента в объеме, определяемом совокупностью существенных признаков промышленного образца, нашедших отражение на изображениях внешнего вида изделия, содержащихся в патенте на промышленный образец.

## Статья 1358 ГК РФ. Исключительное право на изобретение, полезную модель или промышленный образец

1. Патентообладателю принадлежит исключительное право использования изобретения, полезной модели или промышленного образца в соответствии со статьей 1229 настоящего Кодекса любым не противоречащим закону способом (исключительное право на изобретение, полезную модель или промышленный образец), в том числе способами, предусмотренными пунктом 2 настоящей статьи. Патентообладатель может распоряжаться исключительным правом на изобретение, полезную модель или промышленный образец.
2. Использованием изобретения, полезной модели или промышленного образца считается, в частности:
  - 1) ввоз на территорию Российской Федерации, изготовление, применение, предложение о продаже, продажа, иное введение в гражданский оборот или хранение для этих целей продукта, в котором использованы изобретение или полезная модель, либо изделия, в котором использован промышленный образец; (далее перечислены еще 4 пункта и дана другая информация).

**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.

**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 оборот 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 изобретения специалистом в данной области техники;
- 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 полезной модели специалистом в данной области техники;
- 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 оборот 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.**

## **Статья 147 УК РФ. 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.**

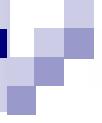
**Лицо, ставшее добросовестно и независимо от других обладателей секрета производства обладателем сведений, составляющих содержание охраняемого секрета производства, приобретает самостоятельное исключительное право на этот секрет производства.**

**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, гарантитные 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.**

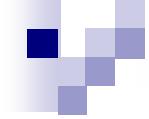


**Заявка на товарный знак должна содержать:**

- **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.**

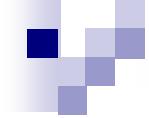
К заявке на товарный знак должны быть приложены:

- **документ, подтверждающий уплату пошлины** за подачу заявки в установленном размере;
- **устав коллектичного 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.

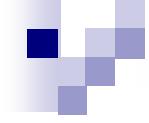
**Исключительное право использования наименования места происхождения товара, предоставляется на основе его регистрации** федеральным органом исполнительной власти по интеллектуальной собственности.

**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 браных 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:

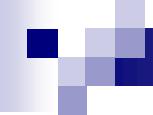
- **создавать впечатление** о том, что они являются лекарственными средствами и (или) обладают лечебными свойствами;
- **содержать ссылки** на конкретные случаи излечения людей, улучшения их состояния в результате применения таких добавок;
- **содержать выражение благодарности** физическими лицами в 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.

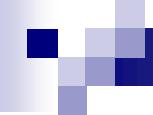
К таким сведениям относятся: характеристики товара, состав и способ изготовления, место происхождения, знаки соответствия госстандартам, возможность приобретения товара в указанном объеме в период времени и в месте, стоимость товара на момент распространения рекламы, наличие у товара официальных наград, призов, дипломов, использование терминов в превосходной степени (лучший, абсолютный, единственный).

**Неэтичная 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 неэтичной 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 осуществляет  
федеральный антимонопольный орган.**

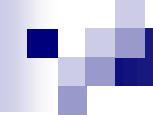
**Таким органом в настоящее время является  
Федеральная антимонопольная служба (ФАС).**

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.

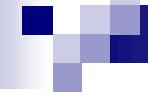
**Фас осуществляет контроль за соблюдением законодательства о рекламе, в том числе:**

- предупреждает, выявляет и пресекает нарушения физическими или юридическими лицами законодательства РФ о рекламе;**
- возбуждает и рассматривает дела по признакам нарушения законодательства РФ о рекламе.**



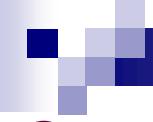
В статье 35 указаны **обязанности антимонопольного органа по соблюдению коммерческой, служебной и иной охраняемой законом тайны.**

**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

## **Защита 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?**

# **Организационное и правовое обеспечение информационной безопасности**

**Доцент кафедры БИТ**

**к.т.н.**

**Струков Владимир Ильич**

## Вопросы к теме 10 ч. 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.

## **11. Правовое обеспечение информационной безопасности РФ**

### **11.1. Концепция национальной безопасности**

**Правовое обеспечение информационной безопасности РФ  
основано на следующих документах:**

**Концепции национальной безопасности РФ**, утвержденной  
Указом Президента РФ от 17 декабря 1997 г. №1300.

**(утратил силу по Указу Президента РФ от 12 мая 2009 года № 537)**

**Доктрине информационной безопасности РФ**,  
утверженной Указом Президента РФ от 5 декабря 2016 г.  
№ Пр-646.

**Стратегии национальной безопасности РФ**, утвержденной  
Указом Президента РФ от 31 декабря 2015 г. № 683.

**Концепция национальной безопасности РФ –  
система взглядов на обеспечение  
безопасности личности, общества и  
государства от внешних и внутренних  
угроз.**



**В настоящее время проявляется тенденция создания структуры международных отношений, основанной на доминировании западных стран при лидерстве США и рассчитанной на военно-силовые, решения ключевых мировых проблем.**

**Национальные интересы России - это баланс интересов личности, общества и государства в экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других сферах.**

**Интересы личности** состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности, в **повышении качества и уровня жизни**, в физическом, духовном и интеллектуальном развитии человека.

**Интересы общества** состоят в упрочении демократии, в **создании правового, социального государства**, в достижении и поддержании общественного согласия, в **духовном обновлении России**.

**Интересы государства** состоят в незыблемости конституционного строя, **суверенитета и территориальной целостности России**, в политической, экономической и социальной стабильности, в обеспечении законности и правопорядка и в развитии международного сотрудничества.

Национальные интересы в духовной сфере состоят в сохранении и укреплении нравственных и духовных ценностей, т.к. их девальвация, представляет собой угрозу федеративному устройству и социально-экономическому укладу РФ.

Национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

## Задачи обеспечения информационной безопасности РФ:

- реализация конституционных прав и свобод граждан РФ в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

**В формировании и реализации политики обеспечения национальной безопасности РФ принимают участие:**

**Президент РФ** – формирует и руководит органами и силами обеспечения национальной безопасности РФ, выступает с посланиями, обращениями и директивами по проблемам национальной безопасности, в своих ежегодных посланиях Федеральному Собранию уточняет отдельные положения Концепции национальной безопасности РФ, определяет направления текущей внутренней и внешней политики страны;

**Федеральное Собрание РФ** - по представлению Президента РФ и Правительства РФ формирует законодательную базу в области обеспечения национальной безопасности РФ;

**Правительство РФ - координирует деятельность федеральных органов исполнительной власти, а также органов исполнительной власти субъектов РФ, формирует статьи федерального бюджета для реализации конкретных целевых программ в этой области;**

**Совет Безопасности РФ - проводит работу по упреждающему выявлению и оценке угроз национальной безопасности РФ, готовит для Президента РФ проекты решений по их предотвращению, разрабатывает предложения в области обеспечения национальной безопасности РФ, а также предложения по уточнению отдельных положений Концепции национальной безопасности РФ, координирует деятельность сил и органов обеспечения национальной безопасности;**

**федеральные органы исполнительной власти -**  
**обеспечивают исполнение законодательства РФ,**  
решений Президента РФ и Правительства РФ в области национальной безопасности РФ; разрабатывают нормативные правовые акты в этой области и представляют их Президенту РФ и Правительству РФ;

**органы исполнительной власти субъектов РФ -**  
**взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения**  
законодательства РФ, решений Президента РФ и Правительства РФ в области национальной безопасности РФ, а также федеральных программ, планов и директив, в области военной безопасности РФ; проводят мероприятия по привлечению граждан, к решению проблем национальной безопасности.

## **11.2. Доктрина информационной безопасности**



**УТВЕРЖДЕНА**  
**Указом Президента РФ**  
**от 9 сентября 2000 г. № Пр-1895**  
**(ред. от 5 декабря 2016 г. № Пр-646)**

**Доктрина развивает  
Концепцию национальной  
безопасности РФ  
применительно  
к информационной сфере.**

**Национальная безопасность РФ зависит от обеспечения  
информационной безопасности, и в ходе технического  
прогресса эта зависимость будет возрастать.**

**Под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью интересов личности, общества и государства.**

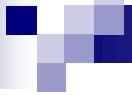
**Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации и ее использования.**

**Интересы общества в информационной сфере  
заключаются в обеспечении интересов  
личности в этой сфере.**

**Интересы государства в информационной сфере  
заключаются в создании условий для  
гармоничного развития российской  
информационной инфраструктуры, в области  
получения информации и пользования ею **в целях**  
обеспечения незыблемости конституционного  
строя, суверенитета и территориальной  
целостности России, **политической,**  
**экономической и социальной стабильности.****

**Выделяются четыре составляющие национальных интересов РФ в информационной сфере:**

- ▶ **1 соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества.**
- ▶ **2 информационное обеспечение государственной политики РФ.**
- ▶ **3 развитие современных информационных технологий.**
- ▶ **4 защита информационных ресурсов и телекоммуникационных систем на территории России.**



## Основные информационные угрозы и состояние информационной безопасности

- возможность **информационно-технического воздействия** на информационную инфраструктуру в военных целях;
- **информационно-психологические воздействия**, направленные на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира;
- **наращивание информационное воздействие** на население России, в первую очередь на молодежь, в целях **размыивания традиционных российских духовно-нравственных ценностей**;
- **рост компьютерных атак** на объекты критической информационной инфраструктуры;

- недостаточный уровень конкурентоспособных информационных технологий для производства продукции и оказания услуг;
- высокий уровень зависимости отечественной промышленности от зарубежных ИТ - электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи;
- недостаточная эффективностью научных исследований, направленных на создание перспективных информационных технологий;
- отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения.

**В РФ реализован следующий комплекс мер по совершенствованию информационной безопасности.**

- Сформирована база правового обеспечения информационной безопасности. (**Приняты Законы “О государственной тайне”, “Об Архивном фонде РФ и архивах”, “Об информации…”, ряд других законов, создаются механизмы их реализации и т.п.**).
- Осуществлены мероприятия по обеспечению информационной безопасности в органах государственной власти, на предприятиях, в учреждениях и организациях независимо от формы собственности.

■ Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов власти.

■ Созданы:

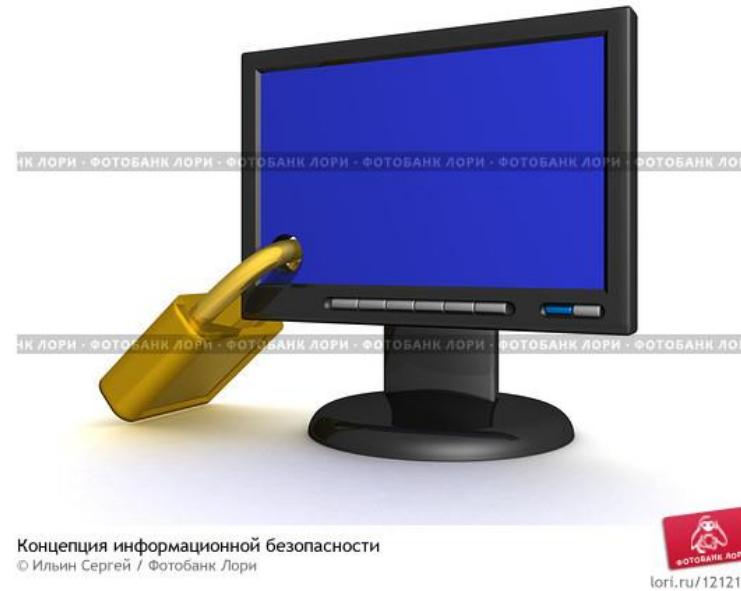
-государственная система

защиты информации,

система защиты ГТ,

-системы лицензирования деятельности в области защиты государственной тайны,

-системы сертификации средств защиты информации.



Концепция информационной безопасности  
© Ильин Сергей / Фотобанк Лори



lori.ru/121218

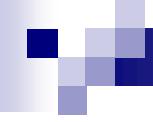
## Недостатки

**Нет четкости при проведении государственной политики в области формирования российского информационного пространства.**

**Недостаточна государственная поддержка российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.**

**Проблемы с обеспечением сохранности сведений, составляющих государственную тайну в результате массового ухода квалифицированных специалистов.**

**Отставание отечественных информационных технологий и как результат - закупки импортной техники, зависимость России от иностранных производителей компьютерной и телекоммуникационной техники.**



В доктрине сделан **общий вывод**

## Уровень информационной безопасности Российской Федерации

в настоящее время

не соответствует потребностям  
общества и государства.

# Методы обеспечения информационной безопасности РФ

В доктрине названы **правовые, организационно-технические и экономические** методы.

К **правовым методам** обеспечения информационной безопасности РФ относится:  
разработка **нормативных правовых актов**,  
регламентирующих отношения в информационной сфере.

# **К организационно-техническими методам**

**относится:**

- **создание и совершенствование системы обеспечения информационной безопасности РФ;**
- **разработка и совершенствование средств защиты информации;**
- **сертификация средств защиты информации, и лицензирование деятельности в области защиты информации.**

## **Экономические методы включают:**

- разработку программ обеспечения информационной безопасности РФ и определение порядка их финансирования;
- создание системы страхования информационных рисков физических и юридических лиц.

**Информационная безопасность РФ оказывает влияние на защищенность национальных интересов РФ в следующих сферах жизнедеятельности:**

- ▶ В экономике.
- ▶ Во внутренней и внешней политике.
- ▶ В области науки и техники.
- ▶ В духовной жизни.
- ▶ В информационных и телекоммуникационных системах.
- ▶ В сфере обороны.
- ▶ В правоохранительной и судебной сферах.
- ▶ В условиях чрезвычайных ситуаций.



Международная конкурентная **борьба** за

-**доминирование на рынках сбыта информационных услуг,**

-**усиление технологического  
отрыва,**

-**создание «информационного  
оружия»,**

**ведет к**

-**гонки вооружений в информационной сфере,**

-**нарастанию агентурного и оперативно-технического  
проникновения** в Россию иностранных разведок, в том  
числе с использованием глобальной информационной  
инфраструктуры.

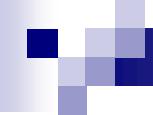
## Основные направления международного сотрудничества Российской Федерации

(в области обеспечения информационной безопасности):

- формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве;
- формирование системы международной информационной безопасности;
- создание международно-правовых механизмов для предотвращения и урегулирования международных конфликтов в информационном пространстве.

# Организационные основы обеспечения информационной безопасности (ИБ)

- Организационную основу системы ИБ РФ составляют:  
Совет Федерации и Государственная Дума,  
Правительство РФ, Совет Безопасности РФ,  
федеральные органы исполнительной власти,  
Центральный банк РФ, Военно-промышленная  
комиссия РФ, межведомственные органы,  
создаваемые Президентом и Правительством РФ,  
органы исполнительной власти субъектов РФ, органы  
местного самоуправления, органы судебной власти,  
принимающие в соответствии с законодательством РФ  
участие в решении задач по обеспечению ИБ.



- Участники системы обеспечения ИБ являются: :
  - собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, СМИ;
  - организации финансового рынка, операторы связи, операторы информационных систем;
  - организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения ИБ, по оказанию услуг в области обеспечения ИБ;
  - организации, осуществляющие образовательную деятельность в данной области.

## **11.3. Стратегия национальной безопасности РФ**

**УТВЕРЖДЕНА  
Указом Президента РФ  
31 декабря 2015 г. № 683**

**Стратегия национальной безопасности - система  
стратегических приоритетов, целей и мер в  
области внутренней и внешней политики,  
определяющих состояние национальной  
безопасности и уровень устойчивого развития  
государства на долгосрочную перспективу.**

## Имеющиеся тенденции и негативные факторы

**Усиление глобального  
информационное противоборства.**

**Развитие, информационных средств  
ведения вооруженной борьбы.**

**Несанкционированная передача за  
рубеж конкурентоспособных  
отечественных технологий.**

**Недостаточное развитие нормативной  
правовой базы.**

**Пропаганда образа жизни, в основе  
которого - вседозволенность и насилие, расовая,  
национальная и религиозная нетерпимость.**

## Интересы обеспечения национальной безопасности требуют:

1. Формирования базовой транспортной, энергетической, информационной и военной инфраструктуры, особенно в

*Арктической зоне,*

*Восточной Сибири,*

*на Дальнем Востоке.*

- 
- 2. Признания первостепенной роли культуры для возрождения культурно-нравственных ценностей.**
  - 3. Создания системы духовного и патриотического воспитания граждан России.**
  - 4. Развития общей гуманитарной и информационно-телекоммуникационной среды.**

## Система документов стратегического планирования

### включает:

- концепцию долгосрочного социально-экономического развития РФ;
- программы социально-экономического развития РФ на краткосрочную перспективу;
- стратегии развития секторов экономики;
- стратегии развития федеральных округов;
- стратегии и комплексные программы социально-экономического развития субъектов РФ;

- межгосударственные программы, в выполнении которых принимает участие РФ,
- федеральные целевые программы,
- государственный оборонный заказ,
- концепции, доктрины и основы государственной политики в сферах обеспечения национальной безопасности и по отдельным направлениям внутренней и внешней политики государства.

## Документы стратегического планирования формируются:

- Правительством РФ,
- федеральными органами исполнительной власти
- органами государственной власти субъектов РФ.

**Информационная и информационно-аналитическая поддержка Стратегии координируется Советом Безопасности РФ с использованием системы распределенных ситуационных центров.**

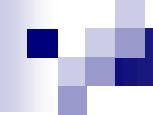
**Для развития системы распределенных ситуационных центров потребуется**

**- преодолеть технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи, определяющих состояние национальной безопасности,**

**- разработать и внедрить технологии информационной безопасности в системах государственного и военного управления, системах управления экологически опасными производствами и критически важными объектами, а также обеспечить условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами.**

## Основные характеристики состояния национальной безопасности включают:

- **уровень безработицы;**
- **децильный коэффициент** (соотношение доходов 10% наиболее и 10% наименее обеспеченного населения);
- **уровень роста потребительских цен;**
- **уровень государственного внешнего и внутреннего долга** в процентном отношении от валового внутреннего продукта;



- **уровень обеспеченности ресурсами**

здравоохранения, культуры, образования и науки в процентном отношении от валового внутреннего продукта;

- **уровень ежегодного обновления вооружения, военной и специальной техники;**

- **уровень обеспеченности военными и инженерно-техническими кадрами.**

## **Контрольные вопросы**

- 1. На каких документах основано правовое обеспечение информационной безопасности РФ?**
- 2. Содержание «Концепции национальной безопасности РФ».**
- 3. Кто занимается формированием и реализацией обеспечением национальной безопасности РФ?**
- 4. Какой документ развивает Концепцию национальной безопасности в информационной сфере?**
- 5. Назовите составляющие национальных интересов РФ в информационной сфере?**
- 6. Укажите методы обеспечения информационной безопасности РФ.**
- 7. Основные положения «Стратегии национальной безопасности РФ».**



# **Организационное и правовое обеспечение информационной безопасности**

**Доцент кафедры БИТ**

**к.т.н.**

**Струков Владимир Ильич**

## **Вопросы к теме 11**

- 1. На каких документах основано правовое обеспечение информационной безопасности РФ?**
- 2. Содержание «Концепции национальной безопасности РФ».**
- 3. Кто занимается формированием и реализацией обеспечением национальной безопасности РФ?**
- 4. Какой документ развивает Концепцию национальной безопасности в информационной сфере?**
- 5. Назовите составляющие национальных интересов РФ в информационной сфере?**
- 6. Укажите методы обеспечения информационной безопасности РФ.**
- 7. Основные положения «Доктрины информационной безопасности РФ».**

## 12. Правовое обеспечение ИБ критически важных объектов и информационно-телекоммуникационных систем

### 12.1. Ключевые системы информационных инфраструктур



**Критически важный объект** - объект, нарушение функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению экономики страны (региона), или существенному ухудшению безопасности жизнедеятельности населения (объект критической информационной инфраструктуры).

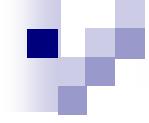
**Из ФЗ США S.773 ("Cybersecurity Act of 2009")**

**"Архитектура национальной цифровой инфраструктуры, базирующейся на Интернете, не защищена и ненадежна. Требуются серьёзные усилия в области безопасности этих систем".**

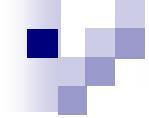
**"Удачные кибератаки на основных финансовых провайдеров могут иметь серьёзные последствия для национальной экономики".**

**"Киберугрозы государственным информационным системам и критическим инфраструктурам эволюционируют и растут".**

**"Наша национальная безопасность и экономика зависят от безопасности, стабильности и целостности коммуникаций и информационной инфраструктуры".**



**Ключевая система информационной инфраструктуры (КСИИ) - это информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация со значительными негативными последствиями.**



## **Критически важная информация –**

**это закрепленная в документации на КСИИ информация, уничтожение, блокирование или искажение которой может привести к нарушению функционирования КСИИ, а также информация о КСИИ (о ее составе, характеристиках управляемого процесса, характеристиках программного и программно-аппаратного обеспечения, размещении, коммуникациях), которая в случае ее хищения (ознакомления с ней) может быть непосредственно использована для деструктивных информационных воздействий на ключевые системы.**



**Перечни критически важных объектов** видов и критически важных систем составляются экспертами и утверждаются органами государственной власти.

### **Признак принадлежности объекта к критически важным-**

- **наличие на объекте экологически опасного или социально значимого производства (процесса),** нарушение штатного режима которого приводит к ЧС,
- **наличие на объекте информационной системы управления чувствительными (важными) для РФ процессами,** нарушение функционирования которой приводит к значительным негативным для страны последствиям.



**В настоящее время совершенствуются методы и способы использования информационных технологий и средств для деструктивных информационных воздействий на информационные ресурсы информационно-телекоммуникационных систем и сетей.**

**Такое применение информационных технологий и средств эквивалентно применению информационного оружия.**

**Для нанесения ущерба интересам государства и общества информационное оружие может быть применено и в мирное время, например, террористическими организациями.**

## **12.2. Правовая база обеспечения безопасности КСИИ**

**Закон №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры РФ».**

**«Основы государственной политики в области обеспечения безопасности населения РФ и защищенности критически важных и потенциально опасных объектов от угроз» (утв. СБ РФ 08.11.2005);**

**«Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий» (утв. СБ РФ 08.11.2005);**

**Распоряжение Правительства от 23.03.2006 №411-рс «Перечень критически важных объектов РФ»;**

**Распоряжение Правительства от 27.08.2005 №1314-р «Об одобрении Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры РФ и опасных грузов»;**

- 
- «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
  - «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
  - «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007);
  - «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007);

**РД ГТК.** Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утв. 30.03.1992);

**РД ГТК.** Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. (утв. 25.07.1997);

**РД ГТК.** Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утв. 4.06.1999).



## Закон «О безопасности критической информационной инфраструктуры РФ» установил:

- ▶ принципы обеспечения безопасности критической информационной инфраструктуры (КИИ),
- ▶ полномочия государственных органов РФ в области обеспечения ее безопасности,
- ▶ права и обязанности субъектов критической информационной инфраструктуры.

В настоящее время действуют также нормы федерального закона от 21 июля 1997 г. ФЗ-№ 116

**«О промышленной безопасности опасных производственных объектов».**



## **Законом были утверждены принципы технического регулирования:**

- лицензирование опасных работ;
- сертификация технических устройств, применяемых на опасных объектах;
- экспертиза и согласование проектов таких объектов;
- выполнение определенного Законом порядка эксплуатации, строительства и приема их в эксплуатацию;
- аттестация персонала в области промышленной безопасности; подготовка к локализации и ликвидации аварий;
- введение объективного производственного контроля за соблюдением требований промышленной и экологической безопасности;
- экспертиза и разработка декларации промышленной безопасности;
- страхование ответственности за причинение вреда.

В соответствии с принятыми Правительством документами в РФ насчитывается более 4600 критически важных и опасных объектов (КВО), которые можно объединить в следующие группы:

- государственные органы управления;
- телекоммуникационные системы;
- водопроводные и сточные системы;
- транспортные системы всех видов, опасные грузы;
- энергетические системы;
- нефтегазовый, топливо-энергетический комплекс;
- химически, биологически опасные объекты;
- аварийные объекты;
- банки.

В 2017 году был также принят закон «**О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации**», в котором указывается, что **информация о мерах по обеспечению безопасности КИИ РФ и о состоянии её защищенности от компьютерных атак относится к сведениям, составляющим ГТ (№187-ФЗ от 26.07.2017).**

В соответствии с требованиями закона, **предприятия и организации должны были провести категорирование своих объектов КИИ и уведомить о результатах ФСТЭК России до января 2019 года.**



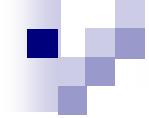
**Целью государственной политики в области мониторинга КВО является уменьшение до приемлемого уровня риска негативного воздействия факторов террористического, техногенного и природного характера на КВО, население страны и окружающую природную среду.**

**Достижение этой цели обеспечивается путём создания федеральной системы мониторинга критически важных и опасных объектов и грузов.**

**Федеральная система мониторинга** критически важных объектов и особо опасных грузов (**ФСМ**) предусматривает следующие **виды мониторинга КВО:**

- 1. Экологический мониторинг**, включая мониторинг природно-климатических факторов и воздействия КВО на окружающую среду (воздух, воду, почву).
- 2. Мониторинг опасных природных процессов:** мониторинг геологических опасных явлений, мониторинг гидрологических опасных явлений, мониторинг метеорологических явлений.

- 
- 3. Техногенный мониторинг**, который включает мониторинг систем технического обслуживания, мониторинг систем инженерных конструкций, мониторинг систем жизнеобеспечения и ЖКХ, мониторинг опасных грузов.
  - 4. Социально-гигиенический мониторинг**: мониторинг состояния здоровья персонала, мониторинг факторов среды персонала; мониторинг социальной среды персонала, мониторинг качества питания и безопасности пищевых продуктов; мониторинг охраны условий труда персонала; мониторинг радиационной обстановки территории.
  - 5. Общественно-политический мониторинг**, включая мониторинг террористических проявлений.



- 6. Информационный мониторинг, мониторинг передачи и защиты информации.**
- 7. Финансово-экономический мониторинг, включая мониторинг уровня износа основных фондов ЖКХ, принадлежащих КВО.**
- 8. Военно-мобилизационный мониторинг.**

**Используются следующие базовые системы для решения задач федеральной системы мониторинга:**

- единая система навигационно-временного обеспечения** РФ, и в первую очередь глобальная космическая навигационная система «ГЛОНАСС»;
- международная система поиска и спасания терпящих бедствие КОСПАС-САРСАТ;**
- системы наблюдения, гидрометеообеспечения и дистанционного зондирования Земли;**
- региональные, ведомственные и объектовые** системы управления, мониторинга, связи и передачи данных.



Структура ФСМ содержит **пять уровней**:

- **федеральный,**
- **межрегиональный,**
- **региональный,**
- **муниципальный,**
- **объектовый.**

На каждом уровне находятся –

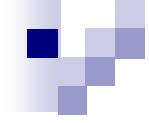
**центры системного мониторинга и оперативного управления, системы, комплексы и средства получения информации об обобщенных параметрах состояния защищенности объектов и грузов.**

## **Зарубежный опыт:**

**-законопроект США «Об информационной безопасности»:**

**Первый раздел** касается работы с персоналом – поиск и приём на работу, разработка должностных обязанностей, повышение квалификации, оценка эффективности и т.д. (Это главное отличие американского документа от всех отечественных нормативных актов, которые о работе с персоналом вообще не говорят).

**Второй раздел** проекта закона касается обязанности президента США разработать долгосрочную национальную стратегию ИБ, предусматривающую множество различных вещей, включая и **измерение эффективности реализации стратегии** (чего нет в российском законодательстве).



**Третий раздел** касается национальной программы повышения осведомленности в области информационной безопасности для всех граждан.

**Четвертый раздел** описывает координацию государства с частным сектором. Для этого создаётся консультационный совет по ИБ, который включает в себя представителей промышленности, академических кругов, некоммерческих организаций, неформальных объединений и других заинтересованных лиц. (Аналог Общественной палаты РФ, являющийся посредником между президентом страны и отраслью ИБ во всех её аспектах).



## Контрольные вопросы

1. Дайте определение критически важного объекта и ключевой системы информационной инфраструктуры.
2. Какие документы составляют правовую базу обеспечения безопасности КСИИ в РФ?
3. Какие объекты отнесены Правительством РФ к критически важным?
4. Какова цель государственной политики в области мониторинга КВО?
5. Назовите виды мониторинга КВО, предусмотренные ФСМ?
6. Назовите базовые системы для решения задач ФСМ ОГ.
7. Зарубежный опыт обеспечения информационной безопасности КВО.