

Информационная сфера - одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающихся в адекватном правовом регулировании.



Принятые во второй половине 90-х годов законодательные акты уже не отвечают современному состоянию общественных отношений и реалиям использования информационных технологий и информационно-телекоммуникационных сетей, по отдельным вопросам вступают в противоречие с более поздними актами, тормозят развитие информационного общества.

Нормативная база



Статья 15 Конституции РФ:
«Общепризнанные принципы и нормы международного права и международные договоры РФ являются составной частью ее правовой системы. Если международным договором РФ установлены иные правила, чем предусмотренные законом, то применяются правила международного договора».

Международный уровень

- 1. «Конвенция, учреждающая Всемирную организацию интеллектуальной собственности»** (Стокгольм, 1967. Вступила в силу для СССР 26.04.1970).
- 2. «Всемирная конвенция об авторском праве»** (Женева, 1952. Пересмотрена в Париже 1971. Вступила в силу для СССР 27.05.1973).
- 3. «Бернская конвенция об охране литературных и художественных произведений в редакции 1971 года».** РФ присоединилась 13.03.1995.
- 4. «Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».** Страсбург, 1998. Ратифицирована Законом РФ от 19.12.2005 № 160-ФЗ.
- 5. «Окинавская Хартия глобального информационного общества»**
Окинава. 22 июля 2000 года.
- 6. Декларация принципов. «Построение информационного общества – глобальная задача в новом тысячелетии».** Всемирная встреча на высшем уровне по вопросам информационного общества. Женева. 10.12.2003.
- 7. «Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций»** (Рим, 1961. Вступила в силу для Российской Федерации 26.05.2003).

8. «Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм» (Женева, 1971. Вступила в силу для Российской Федерации 13.03.1995).

9. «Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации» (Минск 1.06.2001)

Ратифицировано Российской Федерацией законом 164-ФЗ от 1.10.2008 г. со следующей оговоркой:

«Российская Федерация оставляет за собой право отказать в исполнении запроса полностью или частично, если исполнение запроса может нанести ущерб ее суверенитету или безопасности.».

Конвенция Совета Европы о компьютерных преступлениях. СДСЕ № 185. (Будапешт. Открыта для подписания 23.11.2001, вступила в силу 1.07.2004. **Не подписана Российской Федерацией**).

ЗАРУБЕЖНЫЕ НОРМАТИВЫ:

«Оранжевая книга» – гос. стандарт США «Критерии оценивания безопасности надежных вычислительных систем» (1984г.);

«Европейские критерии безопасности информационных технологий» (1991 г.)

«Федеральные критерии безопасности информационных технологий» США

«Канадские критерии безопасности компьютерных систем» (1993 г.)

«Единые критерии оценивания безопасности информационных технологий» (Великобритания, Германия, Канада, Нидерланды, США, Франция 1997 г.)

Единый международный стандарт оценивания безопасности информационных технологий (**ISO/IEC 15408: 1999 «Общие критерии»**)

ISO/IEC 15408-2:2002 ISO/IEC 15408-2:2005 ISO/IEC 15408-2:2008

«Общие критерии» обобщили содержание и опыт использования «Оранжевой книги» и ее интерпретаций.

«Общие критерии» - наиболее полная на сегодняшний день совокупность требований безопасности информационных технологий.

Соглашение о взаимном признании оценок, полученных на основе Общих критериев подписали 26 стран (на 31.12.2013 г.).

В рамках Соглашения в 17 странах действуют аккредитованные органы по сертификации.

Аналоги в России: ГОСТ Р ИСО/МЭК 15408:2002 ГОСТ Р ИСО/МЭК 15408:2005
ГОСТ Р ИСО/МЭК 15408:2008

Руководящие документы Гостехкомиссии РФ (ч. 1, 2,3): «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий»
(Введены Приказом Гостехкомиссии от 19.06.2002 г. № 187)

Часть 1 РД определяет виды требований безопасности, основные конструкции представления требований безопасности и содержит основные методические положения по оценке безопасности ИТ.

Часть 2 РД содержит каталог функциональных требований безопасности.

Часть 3 РД содержит каталог требований доверия к безопасности и оценочные уровни доверия.

ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности.

ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования доверия к безопасности

Гостехкомиссией России в 2003 году разработан ряд **методических документов** в соответствии со стандартом ГОСТ Р ИСО/МЭК 15408:

Руководство по разработке профилей защиты и заданий по безопасности

Положение по разработке профилей защиты и заданий по безопасности

Руководство по формированию семейств профилей защиты

Руководство по регистрации профилей защиты

Концептуальные документы РФ

1. **«Конституция Российской Федерации»** от 12.12.1993.
2. **«Доктрина информационной безопасности Российской Федерации»**.
Утверждена Указом Президента РФ от 9.09.2000 № Пр-1895.
3. **«Концепция национальной безопасности Российской Федерации»**
Утверждена Указом Президента РФ от 10.01.2000 № 24.
4. **«Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года»**.
Распоряжение Правительства РФ от 27.09.2004 № 1244-р.
5. **«Концепции создания системы персонального учета населения Российской Федерации»**. Утверждена Распоряжением Правительства РФ от 9.06.2005 № 748-р.
6. **«Концепция региональной информатизации до 2010 года»**.
Одобрена распоряжением Правительства РФ от 17.07.2006 № 1024-р.
7. **«Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»**. Утвержден решением Гостехкомиссии от 30.03.1992.

Концептуальные документы РФ

- 8. Стратегия развития информационного общества в России.**
Утверждена Советом Безопасности Российской Федерации 25.07.2007 г.
- 9. «Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года»,** утверждена распоряжением Правительства РФ от 17.11.2008 г. № 1662-р;
- 10. Об основных направлениях деятельности Правительства Российской Федерации на период до 2012 года** (распоряжением Правительства РФ от 17.11.2008 г. № 1663-р.);
- 11. Государственная Программа Российской Федерации «Информационное общество (2011 - 2020 годы)»** (распоряжением Правительства РФ от 20.10.2010 № 1815-р;
- 12. «Стратегия развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года»**
Распоряжение Правительства от 1.11.2013 г. № 2036-р
- 13. Стратегия национальной безопасности Российской Федерации до 2020 г.**
утверждена Указом Президента РФ № 537 от 12.05.2009 г.
- 14. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года**
(Утверждены Президентом РФ 24 июля 2013 г., № Пр-1753)

Федеральные Законы

1. **«О средствах массовой информации» от 27.12.1991 № 2124-1**
2. **«Об оперативно-розыскной деятельности» от 12.08.1995**
3. **«Уголовный кодекс Российской Федерации» от 13.06.1996**
4. **«О лицензировании отдельных видов деятельности» № 99-ФЗ от 4.05.11**
Утратил силу № 128-ФЗ от 8.08.2001 «О лицензировании отдельных видов деятельности»
5. **«Кодекс РФ об административных правонарушениях» от 30.12.2001**
6. **«Трудовой Кодекс Российской Федерации» от 30.12.2001**
7. **«Об электронной подписи» от 6.04.2011 № 63-ФЗ.**
Утратил силу «Об электронной цифровой подписи» от 10.01.2002.

Федеральные Законы

8. «О техническом регулировании» № 184-ФЗ от 27.12.2002

Утратили силу:

от 10.06.1993 г. № 5151-1 «О сертификации продукции и услуг»

от 10.06.1993 г. № 5154-1 «О стандартизации»

9. «О персональных данных» от 27.07.2006 № 152-ФЗ.

10. «О рекламе» № 38-ФЗ от 13.03.2006

11. О государственной тайне № 5485-1 от 21.07.1993

12. О коммерческой тайне № 98-ФЗ от 29.07.2004

13. «О защите детей от информации, причиняющей вред их здоровью и развитию» № 436-ФЗ от 29.12.2010.

Вступил в силу 1.09.2012.

Федеральные Законы

14. «Гражданский кодекс Российской Федерации» от 30.11.1994

(ч. 4 вступила в силу с 1 января 2008 года)

Утратили силу законы:

от 23.09.1992 № 3520-1 "О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров"

от 23.09.1992 № 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных"

от 23.09.1992 № 3526-1 "О правовой охране топологий интегральных микросхем"

от 9.07.1993 № 5351-1 "Об авторском праве и смежных правах"

от 23.09.1992 № 3517-1 «Патентный закон»

15. «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Утратили силу законы:

«Об информации, информатизации и защите информации» от 20.02.1995

«Об участии в международном информационном обмене» от 4.06.1996

16. «О связи» от 07.07.2003 № 126-ФЗ (ред. от 21.07.2014)

Утратил силу закон «О связи» от 16.02.1995 г. № 15-ФЗ

Структура законодательства в области ИБ:

- об информации, информационных технологиях и защите информации;
- о персональных данных;
- об интеллектуальной собственности;
- о тайнах;
- о средствах массовой информации;
- о связи;
- о техническом регулировании;
- о лицензировании деятельности в области ИБ.
- об электронной подписи.

Нормативная правовая база по каждому направлению состоит из одного или нескольких базовых федеральных законов и нормативных документов органов государственной власти (указов Президента, постановлений правительства, приказов федеральных министерств и ведомств).

Законодательство об информации, информационных технологиях и защите информации.

Базовый закон - № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также ряд других законов и нормативных документов.

Предмет регулирования: отношения, возникающие при осуществлении права на поиск, получение, распространение и защиту информации, применение ИТ.

Цель регулирования: защита прав и свобод человека в области доступа к информации и ИТ, а также ее защиты от НСД.

Ограничение доступа к информации устанавливается только федеральными Законами в целях защиты основ конституционного строя, прав и законных интересов других лиц, обеспечения безопасности государства.

Федеральный Закон 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

Информация - сведения (сообщения, данные) независимо от формы их представления.

Информация в зависимости от категории доступа к ней подразделяется на:

общедоступную;
ограниченного доступа.

Информация в зависимости от порядка распространения подразделяется на:

свободно распространяемую;
информацию, которая в соответствии с федеральными законами
подлежит предоставлению или распространению;
распространение ограничивается или запрещается.

Виды информации ограниченного распространения:

государственная тайна

коммерческая тайна

профессиональная тайна

служебная тайна

информация о частной жизни, личная и семейная тайна

персональные данные

Законодательство о персональных данных.

Базовый закон - № 152-ФЗ «О персональных данных», а также ряд других законов и нормативных документов.

Предмет регулирования: отношения, возникающие при осуществлении обработки этих данных как с применением ИТ, так и без их применения.

Цель регулирования: защита прав и свобод человека при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни.

Основные угрозы безопасности этих прав заключаются в неправомерном использовании собираемых персональных данных операторами (госорганами, юридическими и физическими лицами).

Законодательство об интеллектуальной собственности.

Базовый закон – Гражданский Кодекс РФ (часть 4), а также ряд других законов и нормативных документов, в том числе международных.

Предмет регулирования: отношения, возникающие в связи с правовой охраной интеллектуальных прав на объекты интеллектуальной собственности.

Виды прав:

авторское право;

право смежное с авторским;

патентное право;

право на селекционное достижение;

право на топологию интегральных микросхем;

право на секрет производства (ноу-хау);

право на средства индивидуализации товаров, услуг, юридических лиц, предприятий (фирменное наименование, товарный знак и т.п.);

право на использование результатов интеллектуальной деятельности в составе единой технологии.

Законодательство о тайнах.

Базовые законы – «О государственной тайне», «О коммерческой тайне», а также ряд других законов и нормативных документов.

Предмет регулирования: отношения, связанные с отнесением информации к конкретному виду тайны, распоряжением этой информацией, охраной ее конфиденциальности.

Режим соответствующей тайны образуется совокупностью правовых, организационных, технических и иных мер, принимаемых обладателем информации, по регламентированию порядка отнесения информации к виду тайн, ее распоряжением и обеспечением защиты.

Нормативные акты по видам тайн (более 60):

Гостайна - Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»,
Указ Президента РФ №1203 от 30.11.1995 «Об утверждении Перечня сведений, отнесенных к государственной тайне»

Коммерческая тайна – Закон РФ №98-ФЗ от 29.07.2004 «О коммерческой тайне»

Персональные данные – Закон РФ №152-ФЗ от 27.07.2006 «О персональных данных»

Налоговая тайна – «Налоговый кодекс РФ»

Банковская тайна – Закон РФ от 02.12.1990 №395-1 «О банках и банковской деятельности»

Врачебная тайна – Закон РФ от 21.11.2011 №323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации"

Адвокатская тайна – Закон РФ от 31.05.2002 №63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации"

Тайна связи – Закон РФ от 07.07.2003 № 126-ФЗ "О связи"

Тайна следствия – Уголовно-процессуальный кодекс

Тайна усыновления – Семейный кодекс

Аудиторская тайна – Закон РФ от 30.12.2008 №307-ФЗ "Об аудиторской деятельности"

и др.

Законодательство о техническом регулировании.

Базовый закон – «О техническом регулировании», а также ряд других законов и нормативных документов.

Утратили силу:

от 10.06.1993 г. № 5151-1 «О сертификации продукции и услуг»

от 10.06.1993 г. № 5154-1 «О стандартизации»

Предмет регулирования: отношения, возникающие при:

исполнении *обязательных* требований к продукции, процессам производства, эксплуатации;

исполнении на *добровольной* основе требований к продукции, процессам производства, эксплуатации;

оценке соответствия.

Технический регламент – документ, устанавливающий *обязательные для исполнения* требования к объектам технического регулирования.

Стандарт – документ, в котором в целях *добровольного использования* устанавливаются требования к объектам технического регулирования.

Законодательство о техническом регулировании.

<http://www.gost.ru>

Федеральное агентство по техническому регулированию и метрологии (Росстандарт) ведет свою деятельность в соответствии с Положением, утвержденным постановлением Правительства РФ от 17 июня 2004 г. № 294.

Федеральное агентство по техническому регулир...

Вход Карта сайта En RSS

10 : 49 : 09 436

Поиск...

Электронные услуги | Техническое регулирование | Стандартизация | Метрология | Подтверждение соответствия | Информационные системы

О Росстандарте
Направления
Деятельность
Часто задаваемые вопросы
Общественная приемная
Пресс-служба

Отзывы продукции

Программа "100 лучших товаров России"

Общественный совет

Открытые ДАННЫЕ

РОССТАНДАРТ
Федеральное агентство по техническому регулированию и метрологии

input
process
management
measure
streamline
combining
technology
distinct
increase
performance
time
output
measured 1.9

Составлен первый рейтинг эффективности технических комитетов по стандартизации

Новости

Все новости

13.01.15 В России создается национальная система стандартов в области управления активами

12.01.15 Обозначения на этикетках текстильных изделий стандартизуют по международному образцу

31.12.14 Поздравление Руководителя Росстандарта Алексея Абрамова с Новым годом

13.01.15 Утверждены технические условия производства геосинтетических материалов для дренирования автодорог

12.01.15 Разработаны требования при госзакупках отдельных медицинских электроизделий

31.12.14 Росстандарт информирует об отзыве 591 шасси транспортных средств Isuzu NQR 90

13.01.15 Стартовал прием заявок

12.01.15 Новый стандарт

31.12.14 Росстандарт утвердил

Законодательство о лицензировании деятельности .

Базовый закон – «О лицензировании отдельных видов деятельности», а также ряд других законов и нормативных документов.

Предмет регулирования: регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности.

Лицензирование отдельных видов деятельности осуществляется **в целях** предотвращения ущерба правам, законным интересам, жизни или здоровью граждан, окружающей среде, объектам культурного наследия народов РФ, обороне и безопасности государства, возможность нанесения которого связана с осуществлением юридическими лицами и индивидуальными предпринимателями отдельных видов деятельности.

Законодательство о лицензировании деятельности .

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

Лицензирование в области защиты информации – деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

Сертификация на соответствие требованиям по безопасности информации – форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Требование по защите информации – установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

Декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов (**ГОСТ Р 53114-2008**)

Законодательство о связи.

Базовый закон – «О связи», а также ряд других законов и нормативных документов.

Предмет регулирования: установление правовых основ деятельности в области связи на территории РФ и на находящихся под юрисдикцией РФ территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Цели:

- создание условий для оказания услуг связи на всей территории РФ;
- содействие внедрению перспективных технологий и стандартов;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
- создание условий для обеспечения потребностей в связи для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка.

Законодательство об электронной подписи.

Базовый закон – «Об электронной подписи» от 6.04.2011 № 63-ФЗ.

Предмет регулирования: закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Законодательство о средствах массовой информации и рекламе.

Базовые законы – «О средствах массовой информации» от 27.12.1991 № 2124-1 (ред. от 24.11.2014)

«О рекламе» от 13.03.2006 № 38-ФЗ (ред. от 21.07.2014)

Предмет регулирования: деятельность средств массовой информации и отношения, возникающие в процессе производства, размещения и распространения рекламы.

Закон «О средствах массовой информации» регламентирует правовое положение учредителей, редакций, журналистов, дает определение основных понятий в сфере масс-медиа, описывает права и обязанности журналистов, закладывает основы свободы массовой информации, устанавливает недопустимость цензуры.

«Окинавская Хартия глобального информационного общества» 22.07.2000 г.

Информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века.

Основные принципы:

защита прав интеллектуальной собственности на ИТ;

обязательство правительств использовать только лицензированное программное обеспечение;

защиты частной жизни при обработке личных данных.

Усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства.

Содействовать использованию бесплатного, общедоступного информационного наполнения и открытых для всех пользователей программных средств, соблюдая при этом права на интеллектуальную собственность.

Содействие подготовке специалистов в сфере ИТ, а также в нормативной сфере.

<http://www.russianlaw.net/law/acts/z8.htm>

«Всемирная конвенция об авторском праве»

Постановление Правительства РФ от 3 ноября 1994 г. N 1224

«О присоединении Российской Федерации к Бернской конвенции об охране литературных и художественных произведений от 9 сентября 1886 г., пересмотренной в Париже 24 июля 1971 г. и измененной 2 октября 1979 г., Всемирной конвенции об авторском праве, пересмотренной в г. Париже 24 июля 1971 г., и дополнительным Протоколам 1 и 2, Конвенции от 29 октября 1971 г. об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм».

Каждое Договаривающееся Государство обязуется принять все меры по обеспечению соответствующей и эффективной охраны прав авторов и других лиц, обладающих авторским правом, на литературные, научные и художественные произведения.

Срок охраны произведений, предоставляемой в соответствии с Конвенцией, не может быть короче периода, охватывающего время жизни автора и двадцать пять лет после его смерти.

Конституция Российской Федерации определяет базовые принципы общественных отношений в информационной сфере.

Статья 15. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

Статья 23. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Статья 24. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Статья 29. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Гарантируется свобода массовой информации. Цензура запрещается.

Статья 44. Интеллектуальная собственность охраняется законом.

**ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ (9.09.2000)**

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ.

Национальные интересы РФ в информационной сфере:

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.
2. Информационное обеспечение государственной политики РФ.
3. Развитие современных информационных технологий, отечественной индустрии информации, использования отечественных информационных ресурсов.
4. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ)

Угрозы ИБ РФ:

1. Неисполнение требований федерального законодательства, регулирующего отношения в информационной сфере;
2. Усиление технологической зависимости России в области современных информационных технологий;
3. Противоправные сбор и использование информации, несанкционированный доступ к информации;
4. Внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
5. Разработка и распространение вредоносных программ;
6. Утечка информации по техническим каналам;
7. Нарушение законных ограничений на распространение информации.

О лицензировании отдельных видов деятельности № 99-ФЗ от 4.05.2011

Статья 12. Перечень видов деятельности, на которые требуются лицензии:

- 1) разработка, производство, распространение криптографических средств, информационных систем и телекоммуникационных систем, защищенных с использованием криптографических средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание криптографических средств, информационных систем и телекоммуникационных систем, защищенных с использованием криптографических;
- 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;
- 4) разработка и производство средств защиты конфиденциальной информации;
- 5) деятельность по технической защите конфиденциальной информации.

Постановление Правительства РФ от 21.11.2011 № 957 (ред. от 28.10.2013)
«Об организации лицензирования отдельных видов деятельности»

ФСБ России:

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.

Разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации.

Деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд).

Постановление Правительства РФ от 21.11.2011 № 957 (ред. от 28.10.2013)
«Об организации лицензирования отдельных видов деятельности»

ФСБ России, ФСТЭК России:

Разработка и производство средств защиты конфиденциальной информации

Примечание:

ФСБ лицензирует разработку средств, устанавливаемых на объектах Администрации Президента, Совета Безопасности, Федерального Собрания, Правительства, Конституционного Суда, Верховного Суда и Высшего Арбитражного Суда Российской Федерации.

(Пост. Правит. РФ № 171 от 3.03.2012)

ФСТЭК России

Деятельность по технической защите конфиденциальной информации

Постановление Правительства РФ от 26.06.1995 № 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»

Утверждено «Положение о сертификации средств защиты информации»

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, а также средства контроля эффективности защиты информации являются средствами защиты информации.

Указанные средства подлежат обязательной сертификации.

При этом криптографические средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ.

Системы сертификации создаются ФСТЭК, ФСБ, Минобороны РФ.

Координацию работ по организации сертификации СЗИ осуществляет Межведомственная комиссия по защите государственной тайны.

Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации»

Органы по сертификации средств защиты информации:

- сертифицируют СЗИ, выдают сертификаты и ведут их учет;
- приостанавливают либо отменяют действие сертификатов;
- принимают решение о проведении повторной сертификации;
- формируют фонд нормативных документов, необходимых для сертификации.

Испытательные лаборатории проводят сертификационные испытания СЗИ и по их результатам оформляют заключения и протоколы, которые направляют в соответствующий орган по сертификации.

Изготовители производят (реализуют) СЗИ только при наличии сертификата. Изготовители должны иметь лицензию на соответствующий вид деятельности.

Информационное сообщение ФСТЭК от 7 апреля 2014 г. № 240/24/1208 «О применении сертифицированной по требованиям безопасности ОС Windows XP в условиях прекращения поддержки разработчиком».

С 8.04.2014 г. прекращается поддержка и выпуск обновлений операционной системы Windows XP.

Органам гос. власти и организациям, использующим для защиты информации версии ОС Windows XP, рекомендуется:

1. Спланировать мероприятия по переводу **до декабря 2016 г.** ИС на сертифицированные ОС, поддерживаемые их производителями.
2. До перехода на сертифицированные ОС принять дополнительные меры защиты:
 - установить все актуальные сертифицированные обновления ОС Windows XP;
 - установить запрет на автоматическое обновление ОС;
 - обеспечивать периодический контроль механизмов защиты ОС;
 - по возможности исключить подключение к сети Интернет и к ЛВС средств ВТ или сегментов ИС, работающих под управлением ОС Windows XP;
 - обеспечить регулярное резервное копирование информации, ПО и средств ЗИ, содержащихся на СВТ или в сегментах ИС под управлением ОС Windows XP;
 - разработать и внедрить правила и процедуры действий должностных лиц в случае выявления уязвимостей в ОС Windows XP .

Сертифицированные продукты Microsoft

<http://certsys.ru/>

Наименование

Windows XP Professional

Windows Vista Ultimate

Windows Vista Business

Windows Server 2008 R2 Datacenter

Windows Server 2008 R2 (Standard Edition, Enterprise Edition)

Windows Server 2008 R2 с Service Pack 1 (SP1)

Windows Server 2008 Enterprise Edition SP1

Windows Server 2003 Standard Edition

Windows Server 2003 Enterprise Edition

Windows 7 Ultimate Edition

Windows 7 Professional Edition

Windows 7 Enterprise

Windows 7 с Service Pack 1 (SP1)

SQL Server 2005 Standard Edition

SQL Server 2005 Enterprise Edition

Microsoft Windows XP Professional

Microsoft Windows Server Standard Edition 2008

Microsoft Windows Server 2008 Enterprise Edition

Microsoft Windows Server 2008 Datacenter

Microsoft System Center Service Manager 2010 SP1

Microsoft System Center Operations Manager 2007 (SP1)

Microsoft System Center Data Protection Manager 2007 (SP1)

Microsoft System Center Configuration Manager 2007 R2

Microsoft SQL Server 2008 (Enterprise Edition, Standard Edition)

Microsoft SharePoint Server 2010 Standard, Enterprise Service Pack 1 (SP1)

Microsoft Office Professional Plus 2007

Microsoft Office 2010 Professional Plus

Microsoft Office 2007 Standard

Microsoft Office 2007 Professional

Microsoft Office 2003 Professional

Сертификат

Сертификаты № 844/2, 844/3

Сертификат № 1516/2

Сертификат № 1516/2

Сертификат № 2181

Сертификат № 2181

Сертификат № 1928/1

Сертификат № 1929/1

Сертификаты №№ 1017/4, 1017/5

Сертификаты №№ 1017/6, 1017/7

Сертификат № 2180

Сертификат № 2180

Сертификат № 2180

Сертификат № 2180/1

Сертификат № 1319

Сертификат № 1319/1

Сертификат № № 844/2, 844/3

Сертификаты № № 1928, 1928/1

Сертификаты № № 1929, 1929/1

Сертификат № 1930

Сертификат № 2555

Сертификат № 1927

Сертификат № 1931

Сертификат № 1932

Сертификат № 1951

Сертификат № 2700

Сертификат № 1960

Сертификат № 2590

Сертификат № 1923

Сертификат № 1587/1

Сертификат № 1056/1

Сертифицированные продукты Microsoft

<http://certsys.ru/>

Наименование

Microsoft Lync Server 2010 (Enterprise Edition)
Microsoft Forefront Identity Manager 2010
Microsoft Forefront Endpoint Protection 2010
Microsoft Forefront Client Security
Microsoft Exchange Server 2010 SP1 (Standard, Enterprise)
Microsoft Dynamics AX 2012 R2
Microsoft BizTalk Server 2009 Standard, Enterprise Edition
Microsoft System Center Virtual Machine Manager 2008
Internet Security and Acceleration Server 2006
Microsoft Forefront

Сертификат

Сертификат № 2763
Сертификат № 2460
Сертификат № 2685
Сертификат № 1764
Сертификат № 2553
Сертификат № 2916
Сертификат № 2438
Сертификат № 1991
Сертификат № 1386
Сертификат № 1764



СЕРТИФИЦИРОВАННЫЕ
ИНФОРМАЦИОННЫЕ
СИСТЕМЫ

Тел.: +7(495) 229-56-07

ГЛАВНАЯ ДИСТРИБУЦИЯ СЕРТИФИКАЦИЯ ПОДДЕРЖКА ПАРТНЕРАМ О КОМПАНИИ КОНТАКТЫ НОВОСТИ МЕРОПРИЯТИЯ

Главная

Сертифицированное ПО



Дистрибуция



<http://certifsecurity.ru/>



Имя:
Пароль:
 Запомнить
[Регистрация](#)
[Восстановление пароля](#)

сертифицированные программные продукты

[Главная](#) [Каталог](#) [Информация](#) [Обучение](#) [Партнёры](#) [О нас](#) [Контакты](#)

ОПРОС НЕДЕЛИ

Какой операционной системой вы пользуетесь?

- Windows XP
- Windows 7
- Linux
- Unix
- Другое

[Архив опросов](#)

ДРУГИЕ ОПРОСЫ

[Главная](#)

Добро пожаловать

Федеральное государственное унитарное предприятие «Предприятие по поставкам продукции Управления делами Президента Российской Федерации» (ФГУП «ППП») предоставляет услуги в области защиты информации и аттестации по требованиям безопасности ФСТЭК и ФСБ (в том числе и услуги по реализации требований ФЗ-152 «О персональных данных»), поставляет и производит компьютерную технику (в том числе в защищенном исполнении), а также лицензионное программное обеспечение, в том числе Microsoft, сертифицированное в Системе сертификации средств защиты информации по требованиям безопасности информации №РОСС RU.0001.01БИ00.

Новые дискуссии

[Мг.](#)

[Мг.](#)

[Мг.](#)

ПОДПИСКА

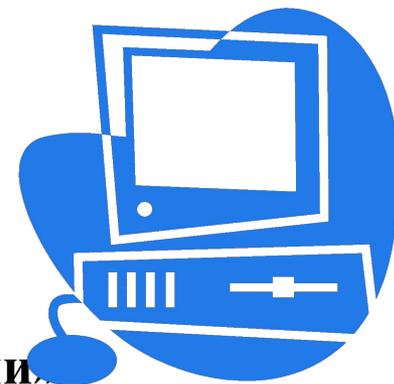
Вы можете бесплатно зарегистрироваться и подписаться на информационное письмо. Каждый месяц Вы будете получать информацию о новых продуктах, прошедших сертификацию и поступивших в продажу, а также дополнительные сведения, недоступные на сайте!

[Архив рассылки](#)

КОРЗИНА ЗАКАЗОВ

Новый базовый Закон

**«Об информации, информационных технологиях
и о защите информации» № 149-ФЗ от 27.07.2006.**



Утратили силу:

**«Об информации, информатизации и защите информации»
№ 24-ФЗ от 20.02.1995**

**«Об участии в международном информационном обмене»
№ 85-ФЗ от 4.06.1996.**

Определяет принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации возникающие при:

- 1) осуществлении права на поиск, получение, передачу, производство и распространение информации;**
- 2) применении информационных технологий;**
- 3) обеспечении защиты информации.**

Не распространяется на отношения, возникающие при правовой охране результатов интеллектуальной деятельности.

№ 149-ФЗ **Основные понятия:**

Информация - сведения (сообщения, данные) независимо от формы их представления;

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 инф. 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 путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

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

Электронный документ - документированная информация, представленная в электронной форме;

Сайт в сети «Интернет» - совокупность программ для ЭВМ и иной информации, содержащейся в ИС, доступ к которой обеспечивается посредством сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»;

Страница сайта в сети «Интернет» - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет";

Доменное имя - обозначение символами, предназначенное для адресации сайтов в сети «Интернет»;

Сетевой адрес - идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

Владелец сайта в сети «Интернет» - лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте;

Провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в ИС, постоянно подключенной к сети «Интернет»

Федеральным законом от 11.07.2011 № 200-ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием закона «Об информации, информационных технологиях и о защите информации» **внесены изменения в 55 законов РФ.**

слова "конфиденциальной информации" заменить словами "информации ограниченного доступа и информации, в отношении которой установлено требование об обеспечении ее конфиденциальности".

слова "конфиденциальной информацией" заменить словами "информацией ограниченного доступа";

Принципы правового регулирования:

- 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 гос. органов;
- 4) равноправие языков народов РФ при создании ИС;
- 5) обеспечение безопасности РФ при создании ИС, их эксплуатации и защите содержащейся в них информации;
- 6) достоверность информации и своевременность ее предоставления;
- 7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних ИТ перед другими.

Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- 2) соблюдение конфиденциальности информации ограниченного доступа;
- 3) реализацию права на доступ к информации.

Обладатель информации, оператор ИС обязаны обеспечить:

- 1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- 2) своевременное обнаружение фактов несанкционированного доступа к информации;
- 3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- 4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- 5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие НСД;
- 6) постоянный контроль за обеспечением уровня защищенности информации;
- 7) нахождение на территории РФ баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ **(вводится с 1.09.2015)**.

**Федеральный закон от 19 декабря 2005 года N 160-ФЗ
«О ратификации Конвенции Совета Европы о защите
физических лиц при автоматизированной обработке
персональных данных»**

**Федеральный Закон от 27 июля 2006 года N 152-ФЗ
«О персональных данных»**

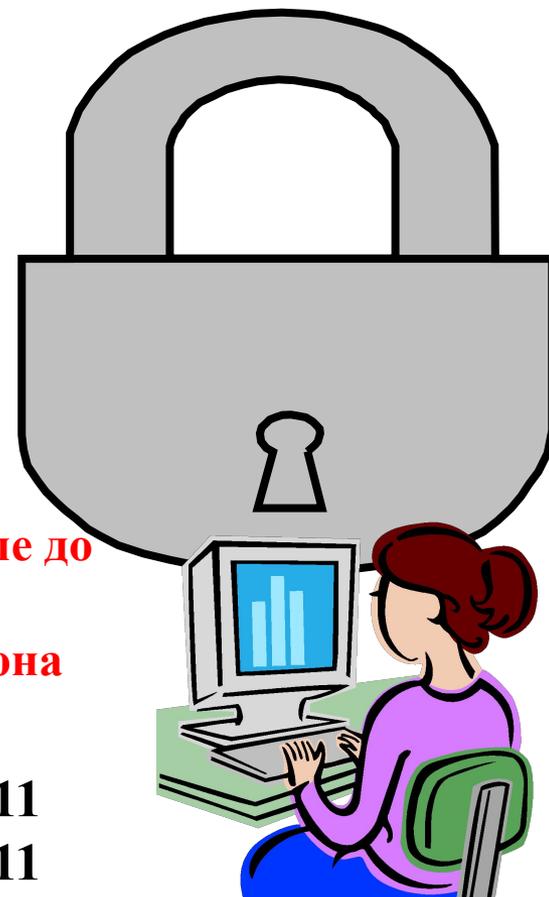
Целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных

Информационные системы персональных данных, созданные до дня вступления в силу закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года.

№ 363-ФЗ от 27.12.2009 – срок до 1.01.2011

№ 359-ФЗ от 23.12.2010 – срок до 1.07.2011



Около 30 нормативных документов (Указы Президента РФ, Постановления Правительства РФ, документы ФСТЭК, ФСБ, Роскомнадзора)

Более 20 Федеральных Законов РФ, затрагивающих вопросы обработки ПД



№ 152-ФЗ Основные понятия:

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПД, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с ПД;

Обработка ПД – любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с ПД, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПД;

Распространение ПД – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

№ 152-ФЗ Основные понятия:

Блокирование ПД – временное прекращение обработки персональных данных;

Уничтожение ПД - действия, в результате которых невозможно восстановить содержание ПД в информационной системе ПД или в результате которых уничтожаются материальные носители персональных данных;

Обезличивание ПД - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному субъекту персональных данных;

Информационная система ПД – совокупность содержащихся в базах данных ПД и обеспечивающих их обработку информационных технологий и технических средств;

Автоматизированная обработка персональных данных – обработка ПД с помощью средств вычислительной техники;

Трансграничная передача ПД – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

№ 152-ФЗ

Согласие в письменной форме субъекта ПД на обработку его ПД должно содержать:

- 1) ФИО, адрес субъекта, данные основного документа (паспорта);
- 2) ФИО, адрес представителя субъекта ПД, данные паспорта, реквизиты доверенности или иного документа, подтверждающего его полномочия;
- 3) Наименование и адрес оператора, получающего согласие субъекта ПД;
- 4) цель обработки персональных данных;
- 5) перечень ПД, на обработку которых дается согласие субъекта;
- 6) наименование и адрес лица, осуществляющего обработку ПД по поручению оператора, если обработка будет поручена такому лицу;
- 7) перечень действий с ПД, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПД;
- 8) срок, в течение которого действует согласие субъекта, а также способ его отзыва;
- 9) подпись субъекта персональных данных.

№ 152-ФЗ

Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом (Ст. 18.1):

- 1) назначение ответственного за организацию обработки ПД;
- 2) издание документов, определяющих политику оператора в отношении обработки ПД, локальных актов по вопросам обработки ПД;
- 3) применение правовых, организационных и технических мер по обеспечению безопасности ПД;
- 4) осуществление внутреннего контроля соответствия обработки ПД закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПД;
- 5) оценка вреда, который может быть причинен субъектам ПД в случае нарушения закона;
- 6) ознакомление работников оператора, непосредственно осуществляющих обработку ПД, с положениями законодательства РФ о персональных данных, в том числе локальными актами оператора по вопросам обработки ПД и обучение указанных работников.

№ 152-ФЗ

Меры по обеспечению безопасности персональных данных при их обработке (Ст. 19):

- 1) определение угроз безопасности ПД при их обработке в ИСПДн;
- 2) применение организационных и технических мер по обеспечению безопасности ПД в ИСПДн;
- 3) применение прошедших процедуру оценки соответствия средств защиты информации;
- 4) оценкой эффективности принимаемых мер по обеспечению безопасности ПД;
- 5) учетом машинных носителей персональных данных;
- 6) обнаружением фактов несанкционированного доступа к ПД и принятием мер;
- 7) восстановлением ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) установлением правил доступа к ПД, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПД;
- 9) контролем за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности информационных систем персональных данных.

№ 152-ФЗ

Уведомление об обработке ПД должно содержать следующие сведения:

- 1) наименование (фамилия, имя, отчество), адрес оператора;
- 2) цель обработки ПД;
- 3) категории ПД;
- 4) категории субъектов, ПД которых обрабатываются;
- 5) правовое основание обработки ПД;
- 6) перечень действий с ПД, описание используемых способов обработки ПД;
- 7) описание мер по обеспечению безопасности ПД;
- 8) дата начала обработки ПД;
- 9) срок или условие прекращения обработки ПД;
- 10) сведения о наличии или об отсутствии трансграничной передачи ПД;
- 10.1) сведения о месте нахождения базы данных информации, содержащей ПД граждан РФ **(вводится с 1.09.2015)**
- 11) сведения об обеспечении безопасности ПД данных в соответствии с требованиями к защите, установленными Правительством РФ (Пост. № 1119).

Орган по защите прав субъектов ПД (Роскомнадзор) имеет право:

- 1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий;
- 2) осуществлять проверку сведений, содержащихся в уведом. об обработке ПД;
- 3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПД;
- 3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства РФ в области ПД; (с 1.09.2015)
- 4) принимать меры по приостановлению или прекращению обработки ПД, осуществляемой с нарушением требований закона;
- 5) обращаться в суд с исковыми заявлениями в защиту прав субъектов ПД;
- 6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии;
- 7) направлять в органы прокуратуры материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПД;
- 8) привлекать к админ. ответственности лиц, виновных в нарушении закона.

№ 152-ФЗ

Вводится с 1 сентября 2015 года:

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной **сети «Интернет»**, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся **на территории Российской Федерации.**

Роскомнадзору дается право ограничивать доступ к информации, обрабатываемой с нарушением законодательства РФ в области ПД.

№ 152-ФЗ

Вводится с 1 сентября 2015 года (в закон 149-ФЗ):

Статья 15.5

В целях ограничения доступа к информации в сети «Интернет», обрабатываемой с нарушением законодательства РФ в области персональных данных, создается автоматизированная информационная система **«Реестр нарушителей прав субъектов персональных данных»**.

В реестр нарушителей включаются:

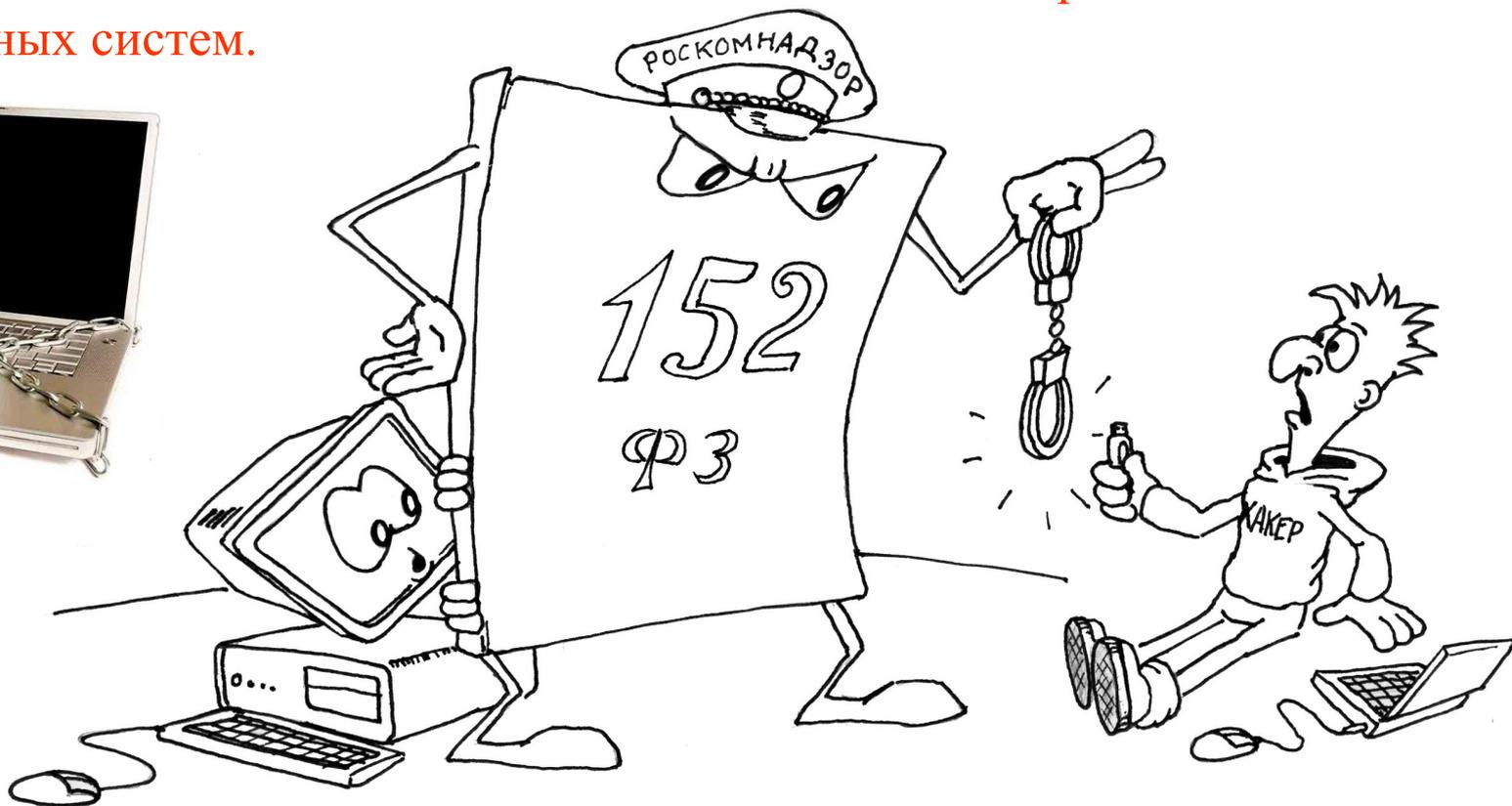
- 1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, обрабатываемую с нарушением законодательства РФ в области персональных данных;
- 2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, обрабатываемую с нарушением законодательства;
- 3) указание на вступивший в законную силу судебный акт;
- 4) информация об устранении нарушения законодательства в области ПД;
- 5) дата направления операторам связи данных об информационном ресурсе для ограничения доступа к этому ресурсу.

Постановление Правительства РФ от 17.11.2007 № 781

«Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Утратило силу

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.



ФСБ и ФСТЭК утвердить в 3-месячный срок нормативные правовые акты и методические документы, необходимые для выполнения требований, предусмотренных Положением.

ФСТЭК февраль 2008 г. документы «ДСП»:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Гриф ДСП снят в ноябре 2009 года.

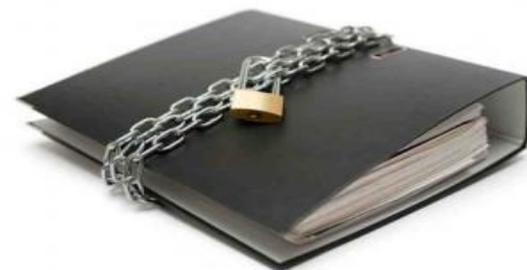
Выписки из первого документа и тексты остальных документов опубликованы на сайте ФСТЭК

Последние 2 отменены

Постановление Правительства РФ от 15.09.2008 № 687

«Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

(Действующий документ)



**«Об утверждении образца формы уведомления об обработке персональных данных»
(приказы Роскомнадзора от 17.07.2008 № 8, от 18.02.2009 № 42)**

Отменены приказом от 16.07.2010 № 482 (новая форма)

Форма изменена приказами Роскомнадзора:

№ 706 от 19.08.2011 (редакция № 37 от 14.03.2014)

№ 346 от 21.12.2011

**Приказ ФСТЭК, ФСБ, Мининформсвязи от 13.02.2008 № 55/86/20
«ПОРЯДОК ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ
ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ»**

Отменен.

**«Положение о методах и способах защиты информации
в информационных системах персональных данных»**

Приказ ФСТЭК России от 5.02.2010 № 58

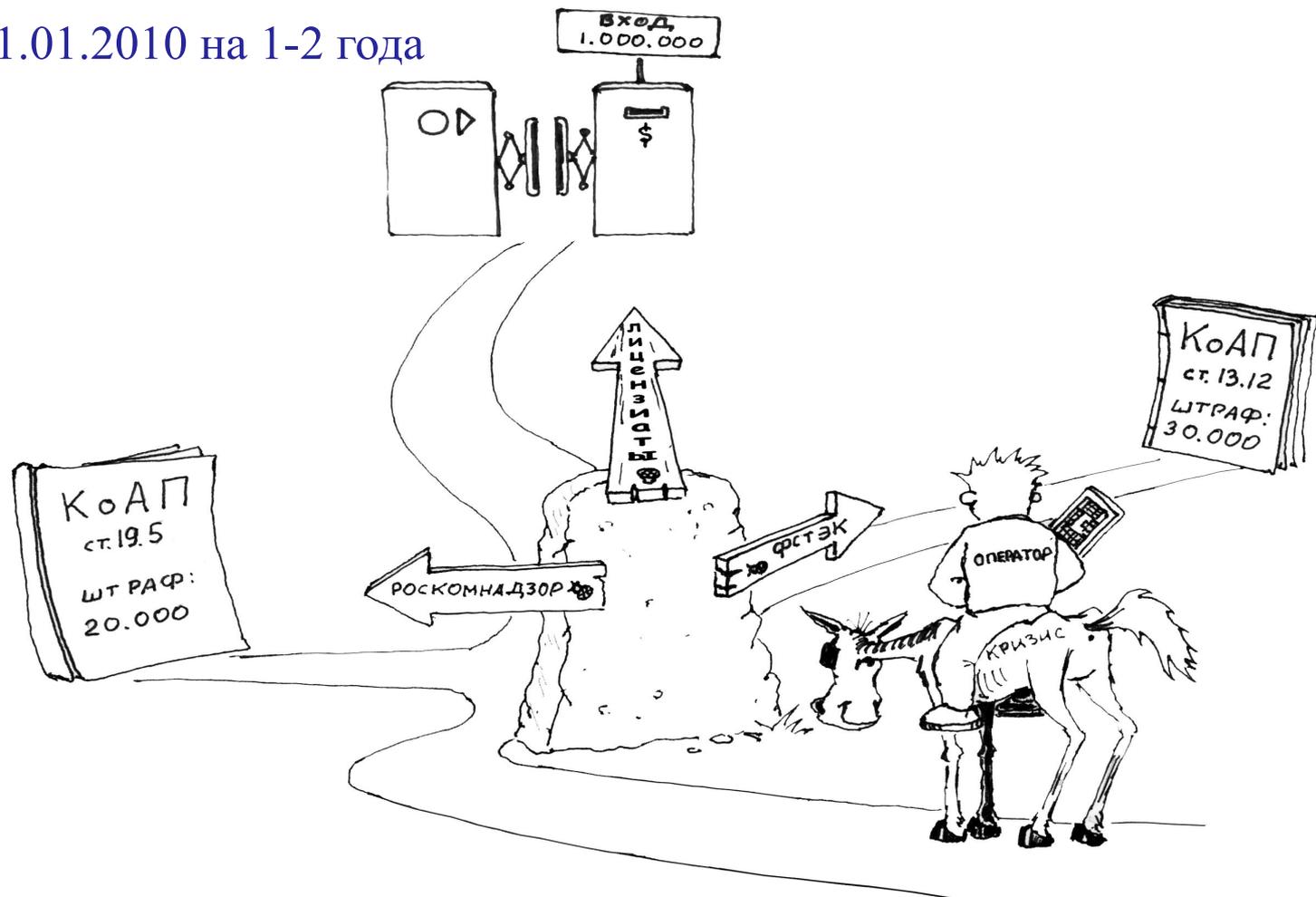
(Отменен приказом № 21 18.02.2013 г.)

Проблемы

1. Гармонизация законодательства (внести поправки в более 20 законов)
2. Совершенствование самого закона 152-ФЗ
3. Разработка и утверждение регламента проведения проверок и контроля за соответствием обработки ПД требованиям законодательства
4. Организация межведомственного взаимодействия МВД, ФСБ, ФСТЭК, прокуратуры и Роскомнадзора по контролю за обработкой ПД
5. Пересмотр документов ФСТЭК и ФСБ в части снижения требований по технической защите информационных систем ПД
6. Обеспечение правоприменительной деятельности в области защиты ПД
7. Хватит ли лицензиатов ФСТЭК на всех операторов?
8. Где взять деньги операторам для защиты ИС ПД во время кризиса?

Парламентские слушания в Госдуме 20.10.2009 г. Рекомендации:

1. Россия после 1.01.2010 столкнется с массовым неисполнением закона
2. Срочно внести поправки в нормативную правовую базу
3. Снизить требования ФСТЭК к технической защите ИСПДн
4. Не применять мер наказания со стороны Роскомнадзора в 2010 году
5. Отсрочить дату 1.01.2010 на 1-2 года



Действующие документы:

Постановления Правительства РФ:

от 15.09.2008 № 687

«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

от 1.11.2012 г. N 1119

«ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»

от 21.03.2012 г. N 211

«ОБ УТВЕРЖДЕНИИ ПЕРЕЧНЯ МЕР, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТЕЙ, ПРЕДУСМОТРЕННЫХ ФЕДЕРАЛЬНЫМ ЗАКОНОМ "О ПЕРСОНАЛЬНЫХ ДАННЫХ» И ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ, ОПЕРАТОРАМИ, ЯВЛЯЮЩИМИСЯ ГОСУДАРСТВЕННЫМИ ИЛИ МУНИЦИПАЛЬНЫМИ ОРГАНАМИ»

от 6.07.2008 г. N 512

«Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Действующие документы:

ПРИКАЗ ФСТЭК от 18 февраля 2013 г. N 21

«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗ ФСБ от 10 июля 2014 г. N 378

«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Приказ Роскомнадзора от 19.08.2011 № 706

"Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных"

Приказ Роскомнадзора от 05.09.2013 № 996

"Об утверждении требований и методов по обезличиванию персональных данных»

Действующие документы:

"Методические рекомендации по применению приказа Роскомнадзора от 5.09.2013 г. № 996 "Об утверждении требований и методов по обезличиванию персональных данных"(утв. Роскомнадзором 13.12.2013)

Приказ Минкомсвязи РФ от 14.11.2011 № 312

"Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных"

Приказ Минкомсвязи России от 21.12.2011 № 346

"Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных".

РОСКОМНАДЗОР – уполномоченный орган по защите прав субъектов персональных данных <http://rkn.gov.ru/>

The image shows two overlapping screenshots of the website of the Federal Service for Supervision of Communications, Information Technologies and Mass Communications (Roskomnadzor). The top screenshot displays a news article dated January 19, 2015, with the headline "19 января Роскомнадзор публикует карты покрытия магистральных дорог федерального значения сетями мобильной связи". The bottom screenshot shows the main page of the "Portal for Personal Data Protection" (Портал персональных данных), which includes a navigation menu on the left, a central content area with the title "Портал персональных данных", and a right sidebar with a "Сформировать обращение" button and contact information for the call center (+7(495)987-68-00).

19 января 2015 года 12+

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

Версия для слабовидящих | En

РОСКОМНАДЗОР

Массовые коммуникации | Связь | Персональные данные | Информационные технологии | Государственные услуги

19 января
Роскомнадзор публикует карты покрытия магистральных дорог федерального значения сетями мобильной связи

19 января 2015 года 12+

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

Версия для слабовидящих | En

РОСКОМНАДЗОР

Массовые коммуникации | Связь | Персональные данные | Информационные технологии | Государственные услуги

О Роскомнадзоре
Новости
Пресс-центр
Государственная служба
Планирование, отчеты о деятельности
Конкурсы и тендеры
Правовая информация
Требования к подконтрольным субъектам
Противодействие коррупции
Обращения граждан и

Главная страница > Персональные данные

Портал персональных данных

[Версия для печати](#)

На [Портале персональных данных Уполномоченного органа по защите прав субъектов персональных данных](#) размещается информация по всему спектру деятельности Роскомнадзора в сфере защиты прав субъектов персональных данных - новости, аналитические материалы, нормативно-распорядительные документы, рекомендации для операторов персональных данных и т.д. Также через Интернет-портал осуществляется доступ к реестру операторов, осуществляющих обработку персональных данных.

Поделиться: [В](#) [f](#) [t](#) [u](#)

Время публикации: 06.10.2009 14:44

Сформировать обращение

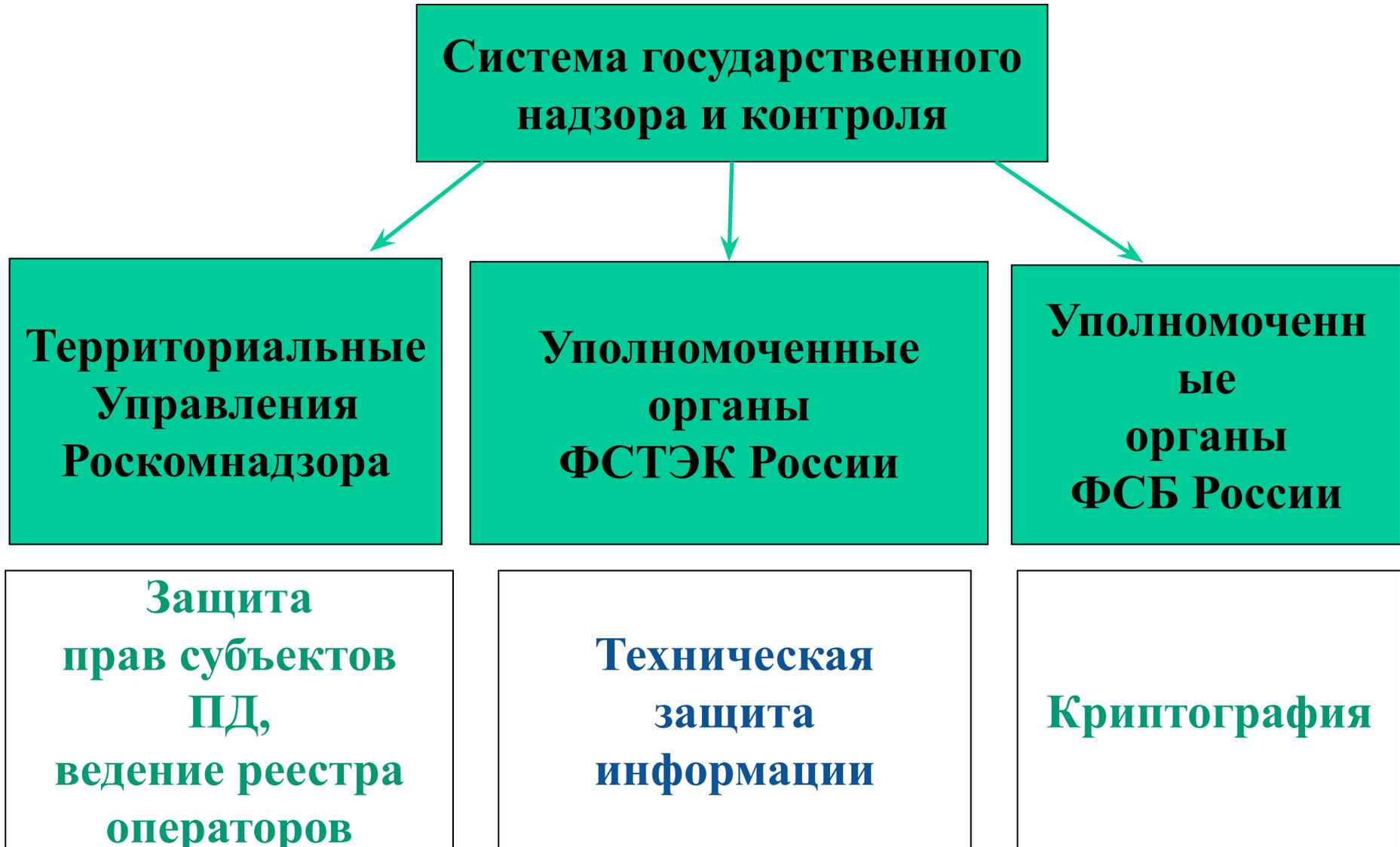
Справочно-информационный центр

Часы работы
Пн-Чт 8:30-17:30
Пт 8:30-16:15

+7(495)987-68-00

Портал персональных данных

Государственный надзор и контроль за обработкой ПД



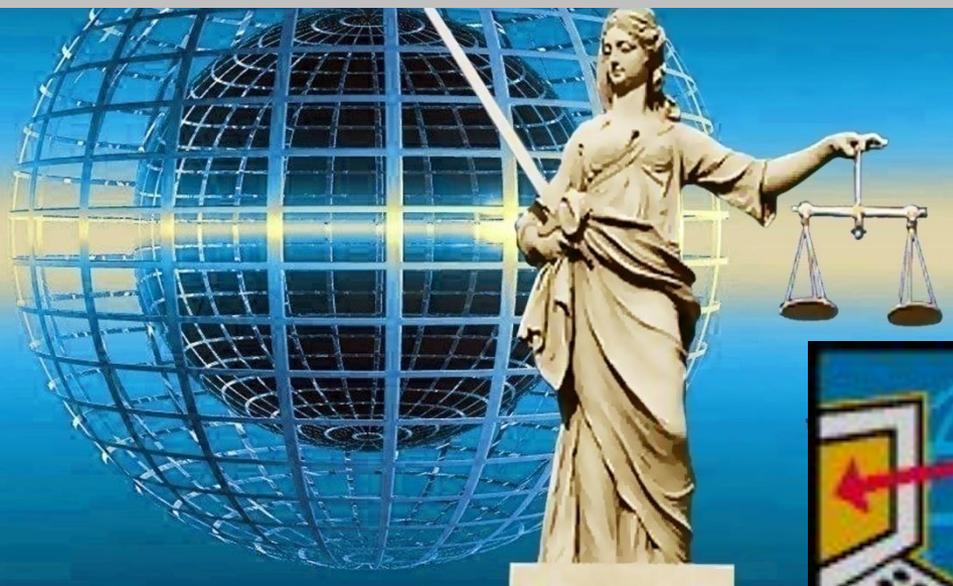
Организация взаимодействия при защите прав субъектов персональных данных



**Федеральный закон «О связи» № 126-ФЗ от 7.07.2003
С поправкой от 09.02.2007 № 14-ФЗ**

**Он заменил собой ранее действовавший Закон «О связи»
от 16.02.1995 N 15-ФЗ.**

**Одной из целей закона является создание условий для развития
российской инфраструктуры связи, обеспечение ее интеграции с
международными сетями связи**



**Гражданский Кодекс. Часть 4.
Принята федеральным законом № 230-ФЗ от 18.12.2006**

**В соответствии с законом № 231-ФЗ от 18.12.2006
Часть 4 ГК вступила в силу с 1 января 2008 года.**

Утратили силу:

«О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» от 23.09.1992 № 3520-1

«О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992 № 3523-1

**«О правовой охране топологий интегральных микросхем»
от 23.09. 1992 года № 3526-1**

**«Об авторском праве и смежных правах»
от 9.07.1993 № 5351-1**

«Патентный закон» от 23.09.1992 № 3517-1



Указ Президента РФ от 24 мая 2011 года № 673 « О Федеральной службе по интеллектуальной собственности»

Постановление Правительства РФ от 21.03.2012 № 218 «О Федеральной службе по интеллектуальной собственности»

<http://www.rupto.ru/>



Федеральная служба по интеллектуальной собственности (Роспатент)



[eng](#) [О Роспатенте](#) [Деятельность](#) [Госзакупки](#) [Госслужба](#) [Нормативно-правовые акты](#) [Пресс-центр](#) [Прием обращений](#) [Ссылки](#)

Размещено [сообщение о признании действия исключительных прав](#) на территории Российской Федерации

25 декабря
2014

Размещен [план проведения конференций и семинаров](#) в регионах Российской Федерации в 2015 г.

25 декабря
2014

15 декабря 2014 г. к поисковой системе Designview [присоединились](#) ведомство по интеллектуальной собственности Республики Корея (KIPO) и патентное ведомство Ирландии (IPO)

22 декабря
2014

С 23 по 27 ноября 2014 г. в г. Женеве (Швейцария) в штаб-квартире ВОИС [состоялась 32-я сессия](#) Постоянного комитета по законам о товарных знаках, промышленных образцах и географических указаниях

17 декабря
2014

11 декабря 2014 г. в [Роспатенте](#) [состоялся](#) «Семинар для представления и обсуждения результатов сравнительного анализа положений законодательных актов ЕС и части IV Гражданского кодекса Российской Федерации в области товарных знаков и промышленных образцов»

16 декабря
2014

Опубликован [пресс-релиз](#) о встрече с представителями Межпрофессионального комитета Шампани (CIVC), Франция

[home](#) [mail](#) [rss](#) [рус](#) [eng](#) [вход](#)

[Версия для слабовидящих](#)

поиск по сайту

[КОНТАКТЫ](#)

[ОТВЕТЫ НА ВОПРОСЫ](#)

[ОБЪЕКТЫ ПАТЕНТНОГО ПРАВА](#)

[ЗАРУБЕЖНОЕ ПАТЕНТОВАНИЕ](#)

[ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ](#)

[РЕАЛИЗАЦИЯ ФЗ-83](#)

[ОФИЦИАЛЬНЫЕ ПУБЛИКАЦИИ](#)

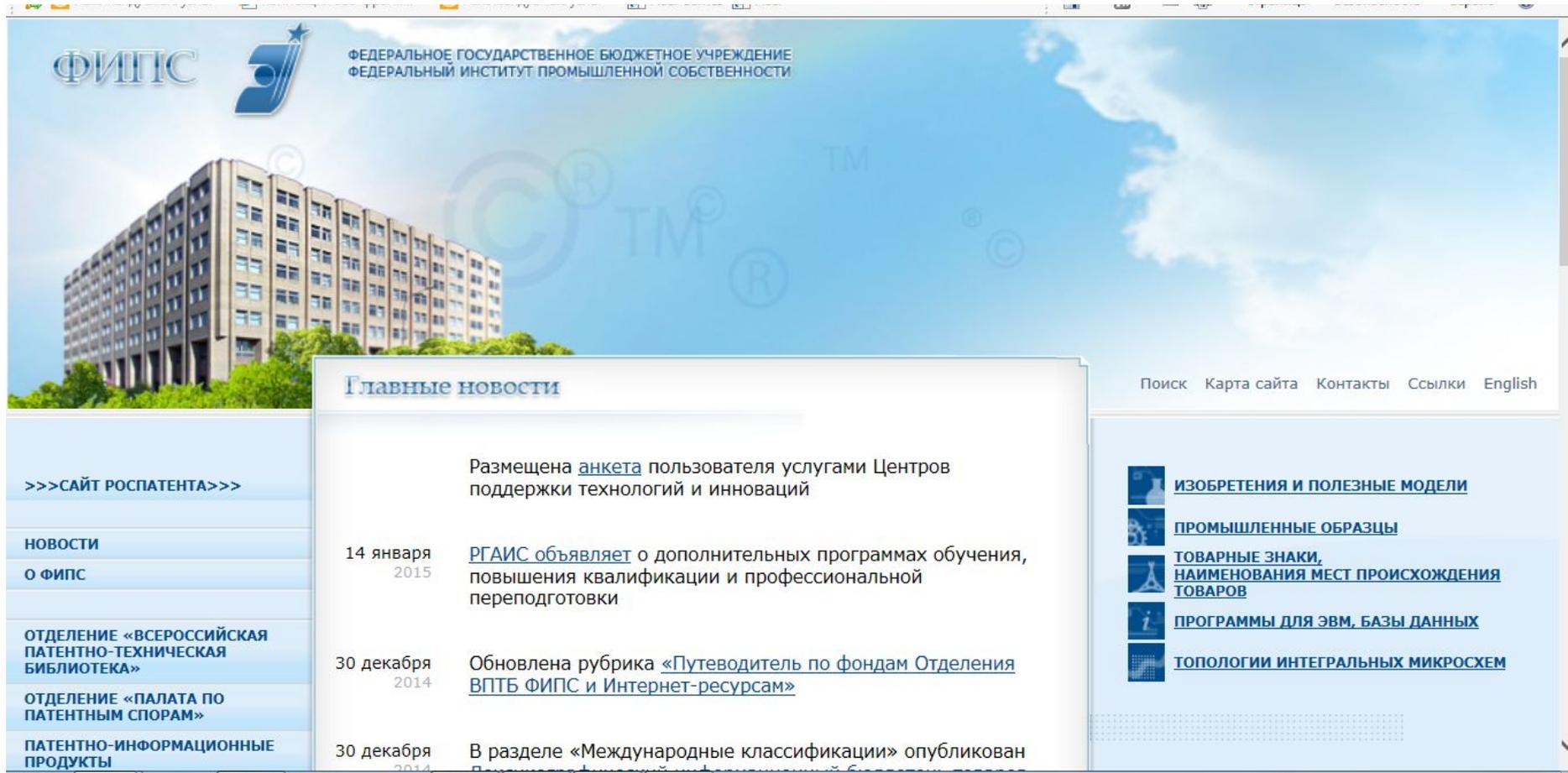
[ИНФОРМАЦИОННЫЕ РЕСУРСЫ](#)

[РОСПАТЕНТ В СИСТЕМЕ «ОТКРЫТОЕ ПРАВИТЕЛЬСТВО»](#)

Регистрация прав на программы для ЭВМ и базы данных.

Федеральное государственное бюджетное учреждение
«Федеральный институт промышленной собственности»

<http://www1.fips.ru>



ФИПС ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

Поиск Карта сайта Контакты Ссылки English

Главные новости

>>>САЙТ РОСПАТЕНТА>>>

НОВОСТИ
О ФИПС

ОТДЕЛЕНИЕ «ВСЕРОССИЙСКАЯ ПАТЕНТНО-ТЕХНИЧЕСКАЯ БИБЛИОТЕКА»

ОТДЕЛЕНИЕ «ПАЛАТА ПО ПАТЕНТНЫМ СПОРАМ»

ПАТЕНТНО-ИНФОРМАЦИОННЫЕ ПРОДУКТЫ

Размещена [анкета](#) пользователя услугами Центров поддержки технологий и инноваций

14 января 2015 [РГАИС объявляет](#) о дополнительных программах обучения, повышения квалификации и профессиональной переподготовки

30 декабря 2014 Обновлена рубрика [«Путеводитель по фондам Отделения ВПТБ ФИПС и Интернет-ресурсам»](#)

30 декабря 2014 В разделе «Международные классификации» опубликован

ИЗОБРЕТЕНИЯ И ПОЛЕЗНЫЕ МОДЕЛИ

ПРОМЫШЛЕННЫЕ ОБРАЗЦЫ

ТОВАРНЫЕ ЗНАКИ, НАИМЕНОВАНИЯ МЕСТ ПРОИСХОЖДЕНИЯ ТОВАРОВ

ПРОГРАММЫ ДЛЯ ЭВМ, БАЗЫ ДАННЫХ

ТОПОЛОГИИ ИНТЕГРАЛЬНЫХ МИКРОСХЕМ

Гражданский Кодекс. Часть 4.

ПРАВА НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ

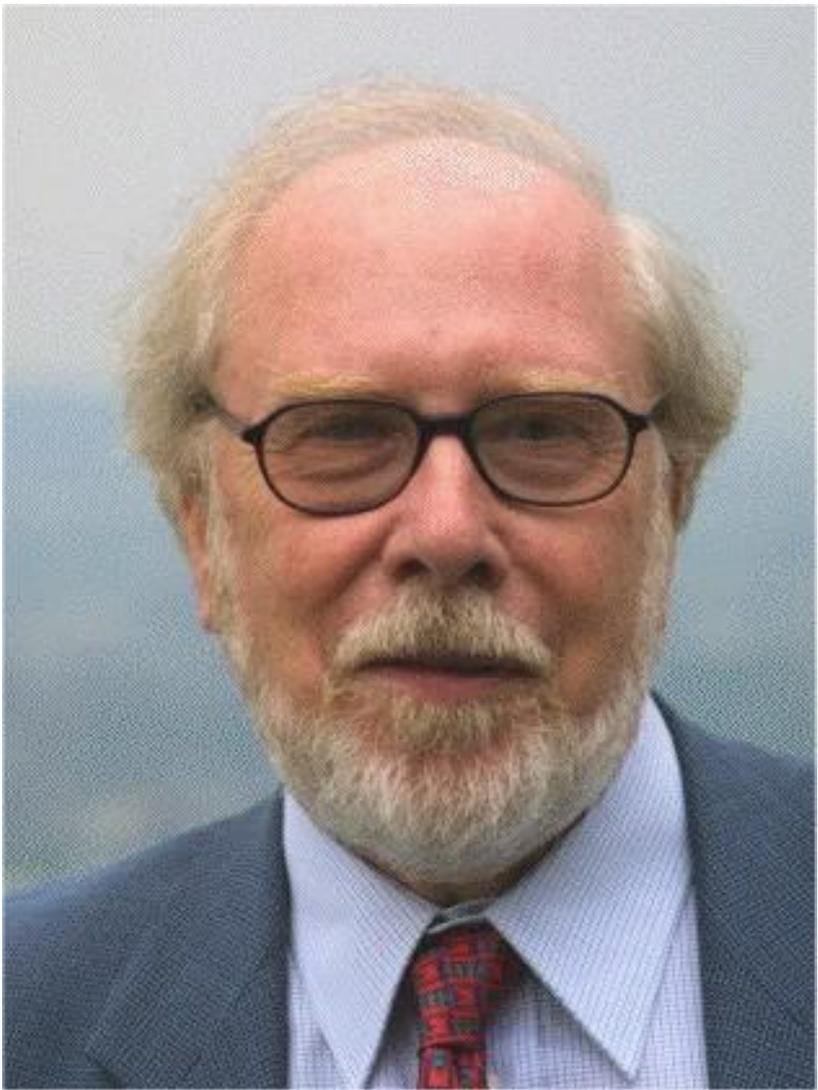


Статья 1225 «Результатами интеллектуальной деятельности, которым предоставляется правовая охрана (интеллектуальной собственностью), являются: произведения науки, литературы и искусства; **программы для ЭВМ; базы данных; фонограммы. . .**»

Статья 1233. Правообладатель может предоставить другому лицу права использования результата интеллектуальной деятельности в установленных договором пределах (**лицензионный договор**).

Статья 1261. 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.

Авторские права на все виды программ для ЭВМ, охраняются так же, как авторские права на произведения литературы.



**«Программирование это не наука,
а искусство!»**

Никлаус Вирт – теоретик в области
разработки языков программирования.

Ведущий разработчик языков Паскаль,
Модула-2, Оберон.

Гражданский Кодекс. Часть 4.

Статья 1262. Правообладатель может по своему желанию зарегистрировать программу или базу данных в федеральном органе исполнительной власти по интеллектуальной собственности.

Статья 1274. Выраженные в цифровой форме экземпляры произведений, предоставляемые библиотеками во временное безвозмездное пользование, могут предоставляться только в помещениях библиотек при условии исключения возможности создать копии этих произведений в цифровой форме.

Статья 1295. Авторские права на произведение науки, литературы или искусства, созданное в пределах установленных для работника (автора) трудовых обязанностей (служебное произведение), принадлежат автору.

Исключительное право на служебное произведение принадлежит работодателю, если трудовым или иным договором между работодателем и автором не предусмотрено иное.

Если работодатель начнет использование служебного произведения автор имеет право на вознаграждение.

Если работодатель в течение трех лет не начнет использование этого произведения, не передаст исключительное право на него другому лицу или не сообщит автору о сохранении произведения в тайне, исключительное право на служебное произведение возвращается автору.

Гражданский Кодекс. Часть 4.

Статья 1296. Исключительное право на программу для ЭВМ, базу данных или иное произведение, созданные по договору, предметом которого было создание такого произведения (по заказу), принадлежит заказчику, если договором между исполнителем и заказчиком не предусмотрено иное.

Автор созданных по заказу программы для ЭВМ или базы данных, которому не принадлежит исключительное право, имеет право на вознаграждение.

Статья 1297. Исключительное право на программу для ЭВМ, базу данных или иное произведение, созданные при выполнении договора подряда либо договора на выполнение научно-исследовательских, опытно-конструкторских или технологических работ, которые прямо не предусматривали создание такого произведения, принадлежит исполнителю, если договором между ним и заказчиком не предусмотрено иное.

Статья 1299. 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.

Гражданский Кодекс. Часть 4.

Статья 1301. В случаях нарушения исключительного права на произведение автор или иной правообладатель наряду с использованием других применимых способов защиты и мер ответственности, установленных Кодексом, вправе требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации:

- 1) в размере от 10000 рублей до 5 млн. рублей, определяемом по усмотрению суда исходя из характера нарушения;
- 2) в двукратном размере стоимости контрафактных экземпляров произведения;
- 3) в двукратном размере стоимости права использования произведения, определяемой исходя из цены, которая обычно взимается за правомерное использование произведения тем способом, который использовал нарушитель.

Статья 1304. Объектами смежных прав являются:

- базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов.

Статья 1311. Ответственность за нарушение исключительного права на объект смежных прав – аналогично ст. 1301.

Гражданский Кодекс. Часть 4.

Статья 1333. Изготовителем базы данных признается лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов. При отсутствии доказательств иного изготовителем базы данных признается гражданин или юридическое лицо, имя или наименование которых указано обычным образом на экземпляре базы данных и (или) его упаковке.

Изготовителю базы данных принадлежат:

- исключительное право изготовителя базы данных;
- право на указание на экземплярах базы данных и (или) их упаковках своего имени или наименования;
- право на обнародование базы данных.

Статья 1334. Никто не вправе извлекать из базы данных материалы и осуществлять их последующее использование без разрешения правообладателя, кроме случаев, предусмотренных настоящим Кодексом.

При этом под извлечением материалов понимается перенос всего содержания базы данных или существенной части составляющих ее материалов на другой носитель с использованием любых технических средств и в любой форме.

Гражданский Кодекс. Часть 4.

Статья 1335. Срок действия исключительного права изготовителя базы данных

1. Исключительное право изготовителя базы данных действует в течение 15 лет.
2. Сроки, предусмотренные п.1 настоящей статьи, возобновляются при каждом обновлении базы данных.

Статья 1335.1. Действия, не являющиеся нарушением исключительного права изготовителя базы данных (введена 12.03.2014 № 35-ФЗ)

Лицо, правомерно пользующееся обнародованной базой данных, вправе без разрешения изготовителя базы данных и в той мере, в которой такие действия не нарушают авторские права изготовителя базы данных и других лиц, извлекать из базы данных материалы и осуществлять их последующее использование:

- в целях, для которых база данных ему предоставлена, в любом объеме, если иное не предусмотрено договором;*
- в личных, научных, образовательных целях в объеме, оправданном указанными целями;*
- в иных целях в объеме, составляющем несущественную часть базы данных.*

Использование извлеченных материалов способом, предполагающим получение к ним доступа неограниченного круга лиц, должно сопровождаться указанием на базу данных, из которой эти материалы извлечены.

Статья 1335.1. Действия, не являющиеся нарушением исключительного права изготовителя базы данных *(продолжение)*

- 2.** Совершение действий другим лицом не считается нарушением права, если это лицо докажет, что оно не могло установить личность изготовителя или оно обоснованно считало, что срок действия исключительного права на базу данных истек.
- 3.** Не допускается неоднократное извлечение или использование материалов, составляющих несущественную часть базы данных, если такие действия противоречат нормальному использованию базы данных и ущемляют необоснованным образом законные интересы изготовителя базы данных.
- 4.** Изготовитель базы данных не может запрещать использование отдельных материалов, хотя и содержащихся в базе данных, но правомерно полученных использующим их лицом из иных, чем эта база данных, источников

Федеральный закон «О коммерческой тайне» № 98-ФЗ от 29.07.2004

Регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность.

Основные понятия:

коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю увеличить доходы, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

информация, составляющая коммерческую тайну

обладатель информации, составляющей коммерческую тайну

доступ к информации, составляющей коммерческую тайну

передача информации, составляющей коммерческую тайну

предоставление информации, составляющей коммерческую тайну

разглашение информации, составляющей коммерческую тайну

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации.

Обладатель информации, составляющей коммерческую тайну, имеет право разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации.

Режим коммерческой тайны не может быть установлен в отношении сведений:

- 1) содержащихся в учредительных документах юридического лица;
- 2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- 3) о составе имущества государственного или муниципального предприятия, и об использовании ими средств соответствующих бюджетов;
- 4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
- 5) о численности, о составе работников, о системе оплаты труда, об условиях труда, и о наличии свободных рабочих мест;

Режим коммерческой тайны не может быть установлен в отношении сведений:

- 6) о задолженности работодателей по выплате заработной платы и иным социальным выплатам;
- 7) о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;
- 8) об условиях конкурсов или аукционов по приватизации объектов;
- 9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников;
- 10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- 11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

Меры по охране конфиденциальности информации:

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- 3) учет лиц, получивших доступ к информации и (или) лиц, которым такая информация была предоставлена или передана;
- 4) регулирование отношений по использованию информации работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- 5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна«

В целях охраны конфиденциальности информации работодатель обязан:

- 1) ознакомить под расписку работника с перечнем информации, составляющей коммерческую тайну;
- 2) ознакомить под расписку работника с установленным режимом коммерческой тайны и с мерами ответственности за его нарушение;
- 3) создать работнику необходимые условия для соблюдения им установленного режима коммерческой тайны.

В целях охраны конфиденциальности информации работник обязан:

- 1) выполнять установленный работодателем режим коммерческой тайны;
- 2) не разглашать эту информацию, без его согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;
- 3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, ставшей ему известной в связи с исполнением им трудовых обязанностей;
- 4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

Нарушение настоящего Федерального закона влечет за собой ответственность:

дисциплинарную (ст. 81 в ТК РФ «разглашение охраняемой законом тайны», ст. 192 «дисциплинарные взыскания»),

гражданско-правовую (ст. 15 ГК «возмещение убытков», ст. 1472 ГК «нарушение исключительного права на секрет производства»),

административную (ст. 13.14 КоАП «Разглашение информации с ограниченным доступом»)

уголовную (ст.183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»)

Федеральный закон «О государственной тайне» № 5485-1 от 21.07.1993

Регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Основные понятия:

государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

носители сведений, составляющих государственную тайну;

система защиты государственной тайны;

допуск к государственной тайне;

доступ к сведениям, составляющим государственную тайну;

гриф секретности;

средства защиты информации;

перечень сведений, составляющих государственную тайну.

Статья 4. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты:

Палаты Федерального Собрания;

Президент Российской Федерации;

Правительство Российской Федерации;

Органы государственной власти РФ, органы государственной власти субъектов РФ и органы местного самоуправления;

Органы судебной власти.

Статья 5. Перечень сведений, составляющих государственную тайну.

1) сведения в военной области

2) сведения в области экономики, науки и техники

3) сведения в области внешней политики и экономики

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с *Перечнем* должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне (*Распоряжение Президента РФ от 16 апреля 2005 г. № 151-пр*).

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах РФ;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами.

Устанавливаются **три степени секретности** сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: **"особой важности"**, **"совершенно секретно"** и **"секретно"**.

На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:

- о степени секретности содержащихся в носителе сведений;
- об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
- о регистрационном номере;
- о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

К органам защиты государственной тайны относятся:

- межведомственная комиссия по защите государственной тайны;
- федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, и их территориальные органы;
- органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

- принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления социальных гарантий;
- ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за его нарушение;
- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Устанавливаются **три формы допуска** к государственной тайне, соответствующие трем степеням секретности: **особой важности, совершенно секретным или секретным.**

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

Уголовный Кодекс РФ:

Статья 275. Государственная измена (*лишение свободы на срок от 12 до 20 лет*)

Статья 276. Шпионаж (*лишение свободы на срок от 10 до 20 лет*)

Статья 283. Разглашение государственной тайны (*лишение свободы на срок от 3 до 8 лет*)

Статья 284. Утрата документов, содержащих государственную тайну (*лишение свободы на срок 3 лет*)

КоАП РФ:

Статья 13.12. Нарушение правил защиты информации

Статья 13.13. Незаконная деятельность в области защиты информации

Статья 13.14. Разглашение информации с ограниченным доступом

Статья 14.49. Нарушение обязательных требований в отношении оборонной продукции

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 **лицензий.**

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

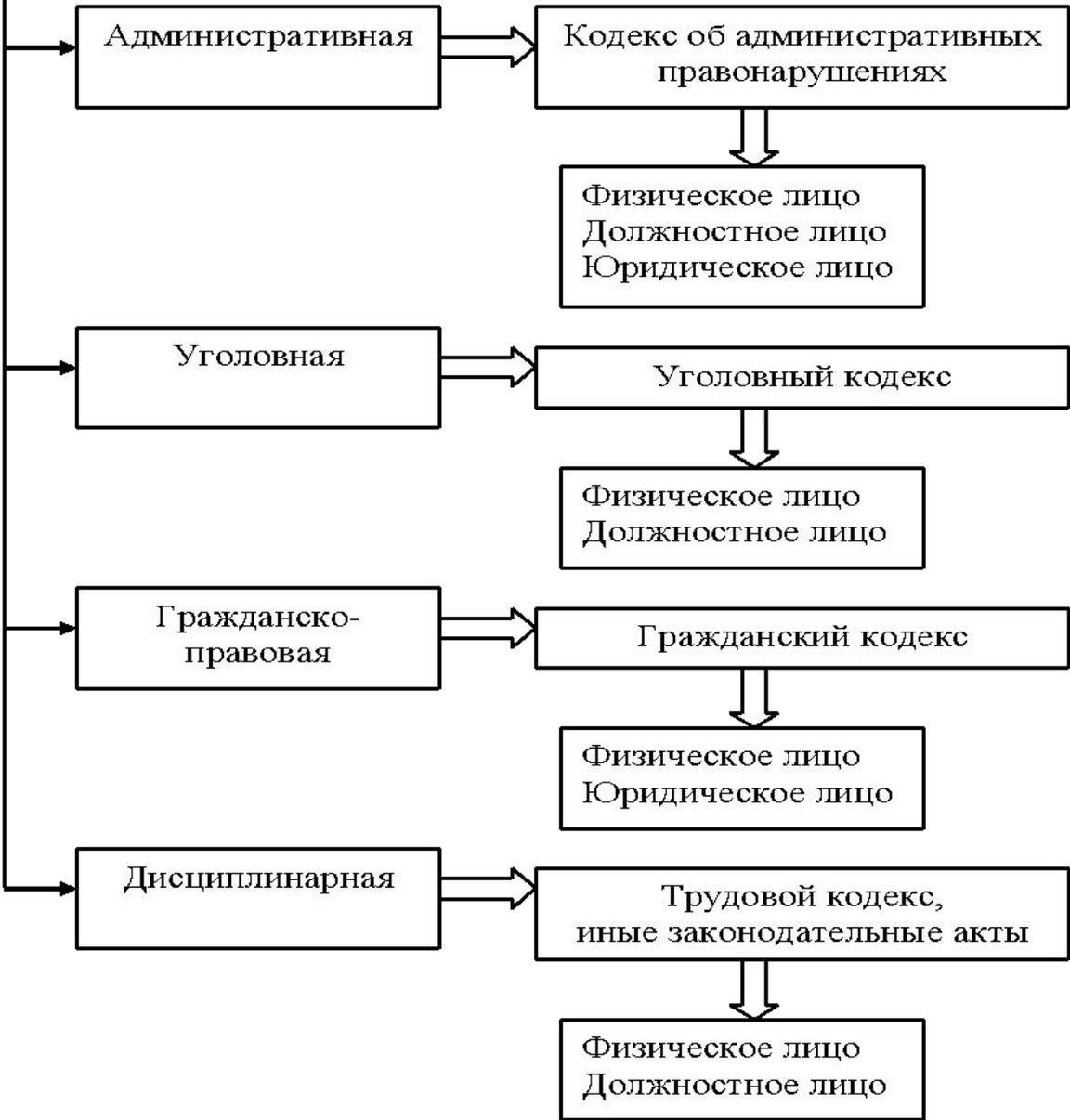
Организация сертификации средств защиты информации возлагается на ФСТЭК, ФСБ, Минобороны (Постановление Правительства РФ от 26.06.1995 г. N 608 «О сертификации Средств защиты информации»).

Координация работ по организации сертификации средств защиты информации возлагается на межведомственную комиссию по защите государственной тайны.

Контроль за обеспечением защиты государственной тайны осуществляют Президент РФ, Правительство РФ.

Надзор за соблюдением законодательства при обеспечении защиты гостайны осуществляет Генеральный прокурор Российской Федерации.

Виды ответственности за нарушения в области ИТ



Правовой акт, статья	Ответчик	Максимальная мера наказания
Кодекс об админ. правонарушениях		
5.27. Нарушение законодательства о труде	Должн.лицо Юрид. лицо	Штраф до 5 тыс. руб. Дисквалифик. до 3 лет Штраф до 50 тыс. руб. Приостан. деят. до 90 сут.
5.39. Отказ в предоставлении гражданину информации	Должностное лицо	Штраф до 1 тыс. руб.
13.11. Нарушение порядка сбора, хранения, использования или распространения перс. данных	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 500 руб. Штраф до 1000 руб. Штраф до 10000 руб.
13.12. Нарушение правил защиты информации	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 1 тыс. руб. Штраф до 4 тыс. руб. Штраф до 30 тыс. руб.
13.13. Незаконная деятельность по защите информации	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 1 тыс. руб. Штраф до 3 тыс. руб. Штраф до 20 тыс. руб.
13.14. Разглашение информации с ограниченным доступом	Физ. лицо Должн. лицо	Штраф до 1 тыс. руб. Штраф до 5 тыс. руб.
19.4. Неповиновение законному распоря-жению органа, осуществляющего гос. надзор	Физ. лицо Должн. лицо	Штраф до 1 тыс. руб. Штраф до 2 тыс. руб.
19.5. Невыполнение в срок законного предписания органа, осуществляющего государственный надзор (Роскомнадзор)	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 500 руб. Штраф до 2 тыс. руб. Дисквалиф. до 3 лет Штраф до 20 тыс. руб.
19.6. Непринятие мер по устранению причин и условий правонарушения	Должностное лицо	Штраф до 500 руб.
19.7. Непредставление или несвоевременное представление сведений в гос. орган	Физ. лицо Должн. лицо Юрид. лицо	Штраф до 300 руб. Штраф до 500 руб. Штраф до 5 тыс. руб.
19.20. Осуществление деятельности без лицензии или с нарушением ее условий	Предприним. Должн. лицо Юрид. лицо	Штраф до 1500 руб. Штраф до 2000 руб. Штраф до 20 тыс. руб.

Кодекс об админ. правонарушениях

Статья 13.31. Неисполнение обязанностей организатором распространения информации в сети «Интернет»

Административный штраф:

1. на граждан - от 1 000 до 3 000 руб.;
на должностных лиц - от 10 000 до 30 000 руб.;
на юридических лиц - от 100 000 до 300 000 руб.
2. на граждан от 3 000 до 5 000 руб.;
на должностных лиц - от 30 000 до 50 000 руб.;
на юридических лиц - от 300 000 до 500 000 руб.
3. на граждан в размере от 3 000 до 5 000 руб.;
на должностных лиц - от 30 000 до 50 000 руб.;
на юридических лиц - от 300 000 до 500 000 рублей.

Кодекс об админ. правонарушениях

Статья 19.7.10. Непредставление сведений или представление заведомо недостоверных сведений в орган (Роскомнадзор)

1. Непредставление или несвоевременное представление провайдером хостинга или иным лицом, обеспечивающим размещение сайта или страницы сайта в сети «Интернет», данных, позволяющих идентифицировать блогера, либо представление в указанный орган заведомо недостоверных сведений - влечет наложение **административного штрафа:**

на граждан от 10 000 до 30 000 руб.;

на юридических лиц от 50 000 до 300 000 рублей.

2. **Повторное** в течение года совершение правонарушения - влечет наложение **административного штрафа:**

на граждан от 30 000 до 50 000 рублей;

на юридических лиц от 300 000 до 500 000 рублей

или приостановление деятельности на срок до тридцати суток.

Кодекс об админ. Правонарушениях

Статья 13.27.1. Нарушение требования о размещении на территории РФ технических средств информационных систем

Нарушение требования, предъявляемого к размещению на территории РФ технических средств ИС, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, -

влечет наложение административного штрафа:

на должностных лиц от 3 000 до 5 000 рублей;

на юридических лиц от 30 000 до 50 000 рублей.

(вступает в силу с 1 июля 2015 года)

Уголовный Кодекс Российской Федерации

Статья 137. Нарушение неприкосновенности частной жизни.

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

Статья 140. Отказ в предоставлении гражданину информации.

Статья 146. Нарушение авторских и смежных прав.

Статья 171. Незаконное предпринимательство (без лицензии).

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.

Уголовный Кодекс Российской Федерации

Правовой акт, статья	Ответчик	Максимальная мера наказания
137. Нарушение неприкосновенности частной жизни	Физическое лицо Должностное лицо	Штраф от 150 до 350 тыс. руб. Лишение права занимать должности до 5 лет. Лишение свободы до 5 лет.
138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации	Физическое лицо Должностное лицо	Штраф от 100 до 300 тыс. руб. Лишение права занимать должности до 5 лет Лишение свободы до 4 лет.
140. Отказ в предоставлении гражданину информации	Должностное Лицо	Штраф до 200 тыс. руб. Лишение права занимать должности до 5 лет.
146. Нарушение авторских и смежных прав.	Физическое лицо Должностное лицо	Лишение свободы на срок до 6 лет Штраф до 500 тыс. руб.
171. Незаконное предпринимательство 171.2. Незаконные организация и проведение азартных игр	Физическое лицо	Штраф до 1 млн.руб. Лишение свободы на срок до 6 лет
183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	Физическое лицо Должностное лицо	Штраф до 200 тыс. руб. Лишение права занимать должности до 3 лет. Лишение свободы до 7 лет.
272. Неправомерный доступ к компьютерной информации	Физическое лицо Должн. лицо	Штраф до 500 тыс.руб. Лишение права занимать должности до 3 лет. Лишение свободы до 7 лет.
273. Создание, использование и распространение вредоносных программ для ЭВМ	Должн. лицо Физическое лицо	Штраф до 200 тыс.руб. Лишение права занимать должности до 3 лет. Лишение свободы до 7 лет.
274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети	Физическое лицо Должн. лицо	Штраф до 500 тыс.руб. Лишение свободы до 5 лет. Лишение права занимать должности до 5 лет.

Уголовный Кодекс Российской Федерации (дополнения)

Статья 185.3. Манипулирование рынком (2010 г.)

(распространение через средства массовой информации, в том числе электронные, информационно-телекоммуникационные сети (включая сеть «Интернет») заведомо ложных сведений)

Штраф от 300.000 до 1 млн.руб., Лишение права занимать должности до 5 лет

Статья 228.1. Незаконные производство, сбыт или пересылка наркотических средств

(с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет", 2013 г.)

Лишение свободы от 15 до 20 лет либо до пожизненного лишения свободы.

Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов (2012)

(с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет")

Лишение свободы от 2 до 6 лет. Лишение права занимать должности до 15 лет

Уголовный Кодекс Российской Федерации (дополнения)

Статья 280. Публичные призывы к осуществлению экстремистской деятельности

(с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет», 2014 г.)

Лишение свободы до 5 лет. Лишение права занимать должности до 3 лет

Статья 280.1. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности РФ

(с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет», 2014 г.)

Лишение свободы до 5 лет. Лишение права занимать должности до 3 лет

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

(с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет», 2014 г.)

Лишение свободы до 5 лет.

Трудовой Кодекс Российской Федерации

Правовой акт, статья	Ответчик	Максимальная мера наказания
81, п.6, пп. в). Разглашение охраняемой законом тайны (ПД)	Должностное лицо	Увольнение
81, п.11. Представление работником работодателю подложных документов при трудоустройстве	Физ. лицо	Увольнение
237. Возмещение морального вреда, причиненного работнику	Юрид. лицо	Размер озмещения определяет суд
391. Неправомерные действия (бездействие) работодателя при обработке и защите ПД	Должн. лицо Юрид. лицо	Меру наказания определяет суд

Трудовой Кодекс Российской Федерации

Правовой акт, статья	Ответчик	Максимальная мера наказания
86. Общие требования при обработке персональных данных работника и гарантии их защиты		
87. Хранение и использование персональных данных работников		
88. Передача персональных данных работника		
89. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя		
90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника		Администрат., уголовная ответств.