ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

О.И. Нестеровский
Н.В. Филиппова

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Воронеж
2019

ББК 32.96

Рецензенты:
В.В. Довгань – начальник отдела защиты информации Центра информационных технологий, связи и защиты информации ГУ МВД России по Воронежской области;
И.А. Домнин – начальник Центра информационных технологий, связи и защиты информации ГУ МВД России по Воронежской области.

Нестеровский, Олег Игоревич. Правовое обеспечение информационной безопасности : учебное пособие [Электронный ресурс] / О.И. Нестеровский, Н.В. Филиппова. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2019. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

Издание содержит основные положения правового обеспечении информационной безопасности Российской Федерации: определено содержание правового обеспечения информационной безопасности, место информационной безопасности в системе национальной безопасности РФ, приведены основные положения законодательства в области обеспечения информационной безопасности РФ. Рассмотрены вопросы правового регулирования защиты государственной тайны, конфиденциальной информации, информационной безопасности в сфере интеллектуальной собственности, а также юридической ответственности за нарушение правовых норм в области информационной безопасности. Представлены тестовые задания для подготовки к промежуточной аттестации.

ISBN 978-5-88591-752-0

Оглавление

ГЛАВА 1. ПОНЯТИЕ И СОДЕРЖАНИЕ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одним из важных вопросов правового обеспечения информационной безопасности является вопрос, связанный с понятийным аппаратом, т.е. с уяснением значения ряда терминов, в частности термина информационная безопасность.

В действующем законодательстве понятие информационной безопасности Российской Федерации установлено Доктриной информационной безопасности, утвержденной Указом Президента № 646 от 5 декабря 2016[1], в соответствии с которой информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Более того, под обеспечением информационной безопасности понимается осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Исходя из данного положения, важной составляющей обеспечения информационной безопасности является правовое обеспечение, которое связано с необходимостью правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации

В большинстве первых отечественных работ правовые меры защиты информации принято рассматривать в рамках организационно-правового обеспечения защиты информации. Объединение организационных и правовых мер вызвано отчасти объективно сложившимися обстоятельствами:

недостаточное количество нормативных, правовых актов, регулирующих вопросы обеспечения информационной безопасности на федеральном уровне;

[1] Доктрина информационной безопасности Российской Федерации : указ Президента РФ от 5 декабря 2016 г. № 646 // Российская газета – 2016. – 6 дек.

преобладающее количество ведомственных нормативных документов, содержащих организационные требования по обеспечению защиты информации;
внедрение автоматизированных информационных систем требовало соответствующего правового обеспечения их защиты, однако на практике в развитии правовой базы долгое время не происходило существенных изменений и приоритет оставался за организационными мерами.

Как следствие указанного положения дел, сложилась такая категория, как *организационно-правовое обеспечение защиты информации*, представляющее собой совокупность законов и других нормативных, правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения защиты информации, так и организацию, и функционирование защиты конкретных объектов и систем.

В настоящее время в связи с пересмотром законодательной базы в сфере информационной безопасности и изданием новых нормативных правовых актов следует говорить именно о правовом обеспечении защиты информации как самостоятельном направлении в структуре комплексной защиты информации.

Правовая защита в указанной области направлена на достижение следующих *целей*:

1) формирование правосознания граждан по обязательному соблюдению правил защиты конфиденциальной информации;

2) определение мер ответственности за нарушение правил защиты информации;

3) придание юридической силы технико-математическим решениям обеспечения защиты информации;

4) придание юридической силы процессуальным процедурам разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

Под *правовым обеспечением информационной безопасности* следует понимать совокупность законов и других нормативных, правовых актов, регламентирующих как общие вопросы обеспечения защиты информации, так и организацию, и функционирование защиты конкретных объектов и систем.

К базовым принципам правового обеспечения информационной безопасности, т.е. основным, исходным идеям, руководящим положениям, которые определяют содержание правового регулирования общественных отношений в области обеспечения информационной безопасности, можно отнести следующее:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, 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 информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Правовое обеспечение информационной безопасности в Российской Федерации как самостоятельной части системы права началось в 1990-х гг., т.е. с момента принятия первых законодательных актов в информационной сфере (Закон РФ от 5 марта 1992 г. № 2446-1 «О безопасности»[1], Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»[2], Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности»[3], в которых закреплялись общие положения правового регулирования общественных отношений по поводу защиты интересов личности, общества и государства в рассматриваемой области.

Однако достаточно стройная система норм права стала складываться после утверждения 9 сентября 2016 г. Президентом РФ Доктрины информационной безопасности Российской Федерации[4].

Правовое обеспечение информационной безопасности любой страны содержит как международные, так и национальные правовые нормы. В Российской Федерации правовые основы обеспечения информационной безопасности составляют Конституция РФ, Законы РФ, Кодексы, Указы и

---

[1] Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

[2] Закон Российской Федерации «О государственной тайне» от 21.07.1993 № 5485-1 (ред. от 18 июля 2009) // Собрание законодательства РФ. - 1997. - № 2

[3]Федеральный закон «О федеральной службе безопасности» от 3 апреля 1995 г. № 40-ФЗ // СЗ РФ. -1995. -№ 15. - Ст. 1269.

[4]Доктрина информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. №646 // Российская газета – 2016. – 6 дек.

другие нормативные акты, регулирующие отношения в области информации.

В системе правовой защиты информации можно выделить 4 уровня.

Первый уровень правовой охраны информации и защиты состоит из международных договоров о защите информации и законов РФ.

Второй уровень правовой защиты информации – это подзаконные акты: указы Президента РФ и постановления Правительства, письма Высшего Арбитражного Суда и постановления пленумов ВС РФ.

Третий уровень - ГОСТы безопасности информационных технологий и обеспечения безопасности информационных систем, также руководящие документы, нормы информационной безопасности и классификаторы, разрабатывающиеся государственными органами.

Четвертый уровень образуют локальные нормативные акты, инструкции, положения по информационной безопасности и документация по комплексной защите информации.

Контрольные вопросы:

1. Что такое информационная безопасность?
2. Что такое правовое обеспечение информационной безопасности?
3. Каково содержание правового обеспечения информационной безопасности?
4. Перечислите уровни системы правовой защиты информации.
5. Раскройте содержание уровней системы правовой защиты информации.
6. Перечислите цели правовой защиты информации.
7. Перечислите принципы правового обеспечения информационной безопасности.

ГЛАВА 2. МЕСТО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РФ

2.1. Безопасность государства: содержание и принципы обеспечения

Основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством, определяет Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» [1].

[1] Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

В соответствии со ст. 2 Федерального закона № 390-ФЗ «О безопасности» основными принципами обеспечения безопасности являются:

соблюдение и защита прав и свобод человека и гражданина;

законность;

системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;

приоритет предупредительных мер в целях обеспечения безопасности;

взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Деятельность по обеспечению безопасности включает в себя:

прогнозирование, выявление, анализ и оценку угроз безопасности;

определение основных направлений государственной политики и стратегическое планирование в области обеспечения безопасности;

правовое регулирование в области обеспечения безопасности;

разработку и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз безопасности, локализации и нейтрализации последствий их проявления;

применение специальных экономических мер в целях обеспечения безопасности;

разработку, производство и внедрение современных видов вооружения, военной и специальной техники, а также техники двойного и гражданского назначения в целях обеспечения безопасности;

организацию научной деятельности в области обеспечения безопасности;

координацию деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области обеспечения безопасности;

финансирование расходов на обеспечение безопасности, контроль за целевым расходованием выделенных средств;

международное сотрудничество в целях обеспечения безопасности;

осуществление других мероприятий в области обеспечения безопасности в соответствии с законодательством Российской Федерации.

Государственная политика в области обеспечения безопасности является частью внутренней и внешней политики Российской Федерации и

представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер. Государственная политика в области обеспечения безопасности реализуется на основе стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов, разрабатываемых Советом Безопасности и утверждаемых Президентом Российской Федерации.

2.2. Стратегия национальной безопасности РФ

Стратегия национальной безопасности Российской Федерации (далее – Стратегия) утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»[1].

Стратегия является базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу.

Правовую основу Стратегии составляют Конституция Российской Федерации, федеральные законы от 28 декабря 2010 г. № 390-ФЗ «О безопасности» и от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации», другие федеральные законы, нормативные правовые акты Президента Российской Федерации.

Стратегия призвана консолидировать усилия федеральных органов государственной власти, других государственных органов, органов государственной власти субъектов Российской Федерации (далее – органы государственной власти), органов местного самоуправления, институтов гражданского общества по созданию благоприятных внутренних и внешних условий для реализации национальных интересов и стратегических национальных приоритетов Российской Федерации.

Стратегия является основой для формирования и реализации государственной политики в сфере обеспечения национальной безопасности Российской Федерации.

Стратегия включает в себя следующие основные разделы:

I. Общие положения.

II. Россия в современном мире.

III. Национальные интересы и стратегические национальные приоритеты.

1 Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации"

IV. Обеспечение национальной безопасности.

V. Организационные, нормативно-правовые и информационные основы реализации настоящей Стратегии.

VI. Основные показатели состояния национальной безопасности.

Основные понятия, вводимые в Стратегии:

«национальная безопасность Российской Федерации» - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее - граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности;

«национальные интересы Российской Федерации» - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития;

«угроза национальной безопасности» - совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам;

«обеспечение национальной безопасности» - реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

«стратегические национальные приоритеты Российской Федерации» важнейшие направления обеспечения национальной безопасности;

«система обеспечения национальной безопасности» - совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов.

В качестве национальных интересов на долгосрочную перспективу в Стратегии определены:

укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;

укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества;

повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны;

сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей;

повышение конкурентоспособности национальной экономики;

закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира.

Обеспечение национальных интересов осуществляется посредством реализации следующих стратегических национальных приоритетов:

оборона страны;

государственная и общественная безопасность;

повышение качества жизни российских граждан;

экономический рост;

наука, технологии и образование;

здравоохранение;

культура;

экология живых систем и рациональное природопользование;

стратегическая стабильность и равноправное стратегическое партнерство.

2.3. Доктрина информационной безопасности РФ

Доктрина информационной безопасности Российской Федерации [1] (далее – Доктрина) утверждена указом Президента РФ от 5 декабря 2016 г. № 646.

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Доктрина служит основой для:

формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

[1] Доктрина информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. №646 // Российская газета – 2016. – 6 дек.

разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Доктрина развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

Доктрина включает в себя следующие основные разделы:

I. Общие положения.

II. Национальные интересы в информационной сфере.

III. Основные информационные угрозы и состояние информационной безопасности.

IV. Стратегические цели и основные направления обеспечения информационной безопасности.

V. Организационные основы обеспечения информационной безопасности.

Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Национальными интересами в информационной сфере являются:

обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации,

Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

Контрольные вопросы:

1. Что относится к основным принципам обеспечения безопасности?
2. Что включает в себя деятельность по обеспечению безопасности?
3. Что представляет собой государственная политика в области обеспечения безопасности?
4. Что является правовой основой Стратегии национальной безопасности Российской Федерации.

5. Раскройте понятие «угроза национальной безопасности».
6. Раскройте понятие «система обеспечения национальной безопасности».
7. Что определяет Стратегия национальной безопасности Российской Федерации в качестве национальных интересов на долгосрочную перспективу?
8. Что относится к национальным интересам в информационной сфере?
9. Что составляет организационную основу системы обеспечения информационной безопасности?
10. На каких принципах основывается деятельность государственных органов по обеспечению информационной безопасности?

ГЛАВА 3. ОСНОВЫ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

3.1. Классификация и структура нормативных правовых актов в сфере обеспечения информационной безопасности

Информационные правоотношения в настоящее время выделяют в самостоятельный вид правоотношений. *Информационные правоотношения* – это отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, а также обеспечении защиты информации

Отрасль законодательства, регулирующая информационные правоотношения, получила название «информационное законодательство» и является самостоятельной в современном российском законодательстве. Информационное законодательство включает:
законодательства об интеллектуальной собственности;
законодательства о средствах массовой информации;
законодательства о формировании информационных ресурсов и предоставлении информации из них;
законодательства о реализации права на поиск, получение и использование информации;
законодательства о создании и применении информационных технологий и средств их обеспечения;
законодательства по защите национальных интересов государства в информационной сфере.

Рассмотрим более подробно классификацию нормативных правовых актов, в совокупности образующих законодательство. Критерием данной классификации является юридическая сила нормативного правового акта.

Нормативный правовой акт – это правовой акт, содержащий нормы права и направленный на урегулирование определенных общественных отношений.

Центральным документом в соответствии с рассматриваемой классификацией занимает закон. *Закон* – это нормативный правовой акт, обладающий высшей юридической силой, выражающий государственную волю по наиболее важным вопросам общественной жизни. Законы принимаются в особом порядке высшими органами власти или непосредственно народом в ходе референдума.

Различают законы: федеральные конституционные, о поправке к Конституции РФ, обычные федеральные, законы субъектов РФ.

Подзаконные акты по общему правилу не должны противоречить законам и должны приниматься во исполнение законов.

Виды подзаконных актов:

1. Акты федеральных органов представительной власти (Постановления Совета Федерации по политическим вопросам).

2. Акты Президента РФ: указы, распоряжения.

3. Акты Правительства РФ (постановления, распоряжения).

4. Акты министерств и ведомств, государственных комитетов, федеральных служб, агентств и т.д. – приказы, инструкции, указания.

5. Акты органов власти и управления субъектов РФ – постановления главы администрации края, области, города. Эти акты имеют локальный характер.

6. Акты государственных и негосударственных организаций – приказ руководителя, устав общественного объединения.

На основании приведенной классификации нормативных правовых актов можно предложить следующую структуру нормативных правовых актов в области информационной безопасности:

1-й уровень – международные правовые акты;

2-й уровень – нормативные правовые акты федерального уровня;

3-й уровень – нормативные акты субъектов Российской Федерации;

4-й уровень – нормативные акты органов местного самоуправления;

5-й уровень – нормативные документы уровня организаций, предприятий, учреждений.

Перечень основных нормативных правовых актов в области информационной безопасности

Международные правовые акты:

Конвенция, учреждающая Всемирную организацию интеллектуальной собственности (Стокгольм, 14 июля 1967 года, в редакции от 2 октября 1979 года. Вступила в силу для СССР 26 апреля 1970 года);

Всемирная конвенция об авторском праве (Женева, 6 сентября 1952 года. Пересмотрена в Париже 24 июля 1971 года. Вступила в силу для СССР 27 мая 1973 года);

Брюссельская конвенция о распространении несущих программы сигналов, передаваемых через спутники. (Конвенция по спутникам), 1974 год. Российская Федерация присоединилась 20 января 1989 года;

Бернская конвенция об охране литературных и художественных произведений в редакции 1971 года. Российская Федерация присоединилась 13 марта 1995 года;

Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. Ратифицирована Законом Российской Федерации от 19 декабря 2005 года №160-ФЗ;

Окинавская хартия глобального информационного общества. Окинава, 22 июля 2000 года;

Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии». Всемирная встреча на высшем уровне по вопросам информационного общества. Женева, 10 декабря 2003 года;

Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций (Рим, 26 октября 1961 года. Вступила в силу в Российской Федерации 26 мая 2003 года);

Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм (Женева, 29 октября 1971 года; вступила в силу для Российской Федерации 13 марта 1995 года);

Всеобщая декларация прав человека от 10.12. 1948;

Соглашения в области информации, заключенные в рамках Содружества Независимых Государств:

Соглашение о сотрудничестве в области информации от 09.10.1992;

Соглашение об обмене правовой информацией от 21.10.1994;

Соглашение о межгосударственном обмене научно-технической информацией от 26.06.1992;

Соглашение о взаимоотношениях министерств внутренних дел в сфере обмена информацией от 24.04.1992.

Нормативные правовые акты федерального уровня:

Конституция Российской Федерации от 12 декабря 1993 г.;

Закон РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации»;

Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне»;

Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности»;

Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»;

Федеральный закон от 10.01.1996 № 5-ФЗ «О внешней разведке»;

Федеральный закон Российской Федерации от 31.05.2002 № 62-ФЗ «О гражданстве Российской Федерации»;

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»;

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;

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

Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;

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

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ;

Гражданский кодекс Российской Федерации (часть первая от 30.11.1994 № 51-ФЗ; часть вторая от 26.01.1996 №14-ФЗ; часть третья от 26.11.2001 № 146-ФЗ; часть четвертая от 18.12.2006 № 230-ФЗ);

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 19.07.2011);

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.

Концептуальные документы:

Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);

Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31.12.2015 № 683);

Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы (утв. Указом Президента РФ от 09.05.2017 № 203);

Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 № Пр-2976).

Указы, Распоряжения Президента Российской Федерации:

Указ Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства,

реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;

Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;

Указ Президента Российской Федерации от 9 января 1996 г. № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации»;

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Положение о Федеральной службе по техническому и экспортному контролю»;

Указ Президента Российской Федерации от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны»;

Распоряжение Президента Российской Федерации от 16 апреля 2005 года № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне»;

Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Указ Президента РФ от 26 февраля 2009 № 228 «Вопросы Межведомственной комиссии по защите государственной тайны».

Постановления Правительства Российской Федерации:

Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»;

Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»;

Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»;

Постановление Правительства РФ от 06 февраля 2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне»;

Постановление Правительства РФ от 03 февраля 2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

Постановление Правительства Российской Федерации от 18 сентября 2006 г. № 573 «О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны»;

Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановление Правительства РФ от 08 февраля 2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

Постановление Правительства РФ от 17 февраля 2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

Постановление Правительства РФ от 08 июня 2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры».

Государственные стандарты:

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России;

ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России;

ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России;

ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Госстандарт России;

ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.

Специальные нормативные документы:

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение председателя Гостехкомиссии России от 30 марта 1992 г.;

Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.;

Руководящий документ. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Сборник руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России, 1998 год;

Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия

недекларированных возможностей. Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114;

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1.Часть 2. Часть 3. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. № 187;

Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год;

Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003 год;

Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 год;

Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 год;

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год;

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год.

3.2. Права и свободы человека и гражданина в сфере информационной безопасности

Понимая все возрастающую роль и место информации в жизни личности, общества, государства, мировое сообщество еще в середине XX столетия ввело правовые механизмы, обеспечивающие гарантии прав и свобод человека и гражданина, значительную роль в которых играют информационные права и свободы.

Информационные права и свободы впервые отражены во Всеобщей декларации прав человека, утвержденной и провозглашенной Генеральной Ассамблеей ООН 10 декабря 1948 г.[1], а именно:

каждый человек должен обладать всеми правами и всеми свободами, провозглашенными настоящей Декларацией, без какого бы то ни было различия, как-то: в отношении расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального

[1] Всеобщая декларация прав человека: [принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.] // Рос. газета. - 1998. - 10 декабря (№ 245). – С. 3.

происхождения, имущественного, сословного или иного положения... (ст.2 Всеобщей декларации);

каждый человек, обвиняемый в совершении преступления, имеет право считаться невиновным до тех пор, пока его виновность не будет установлена законным порядком путем гласного судебного разбирательства, при котором ему обеспечиваются все возможности для защиты (ст. 11 1. Всеобщей декларации);

никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств (ст.12 Всеобщей декларации);

каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ (ст. 19 Всеобщей декларации);

каждый человек имеет право свободно участвовать в культурной жизни общества, наслаждаться искусством, участвовать в научном прогрессе и пользоваться его благами; каждый человек имеет право на защиту его моральных и материальных интересов, являющихся результатом научных, литературных или художественных трудов, автором которых он является (ст. 27 Всеобщей декларации);

ничто в настоящей Декларации не может быть истолковано как предоставление какому-либо государству, группе лиц или отдельным лицам права заниматься какой-либо деятельностью или совершать действия, направленные к уничтожению прав и свобод, изложенных в настоящей Декларации (ст. 30 Всеобщей декларации).

Конвенция Совета Европы о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) [1] развивает положения, закрепляющие информационные права и свободы, так в частности ст.10 1. содержит положение, в соответствии с которым каждый человек имеет право на свободу выражать свое мнение. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны государственных органов и независимо от государственных границ.

Право граждан на информацию закреплено в Конституции РФ. Это закрепление вводит законодательство России в систему международных норм.

[1] Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21 сентября 1970 г., 20 декабря 1971 г., 1 января 1990 г., 6 ноября 1990 г., 11 мая 1994 г.) // Бюллетень международных договоров. - март 2001 г. - №3.

В соответствии с п. 4 ст.29 каждому предоставлено право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. При этом следует отметить, что право свободно искать и получать означает право каждого обращаться к органам государственной власти, общественным объединениям, органам и организациям, частным фирмам, другим структурам по вопросам, затрагивающим основные права и свободы, провозглашенные Конституцией РФ[1], а также получения у них запрашиваемой информации. Право передавать информацию означает право свободного обмена информацией каждого с каждым. Право производить и распространять информацию означает свободу каждого на творчество и интеллектуальную деятельность, сопровождаемую созданием новой или производной информации, а также на свободу широкого распространения произведенной информации всеми законными способами. Эти права могут быть ограничены только законом. Право на получение информации от государственных органов и органов местного самоуправления также закреплено в ст. 33 Конституции РФ:

«Граждане Российской Федерации имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления». Можно добавить – с целью осуществления права на поиск и получение информации.

Право на получение информации от государственных органов и органов местного самоуправления возлагает на эти структуры обязанность по подготовке и предоставлению запрашиваемой информации, что и закреплено в ст. 24 Конституции РФ: «2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы-, если иное не предусмотрено законом». *Более того, ст. 41 Конституции РФ* закрепляет наступление ответственности должностных лиц за сокрытие фактов и обстоятельств, создающих угрозу для жизни и здоровья людей.

Также Конституцией РФ установлена свобода творчества и интеллектуальной деятельности, право на интеллектуальную собственность, полученную в результате творчества, а именно:
каждому гарантируется свобода мысли и слова (ст.29);

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)// Собрание законодательства РФ, 04.08.2014, № 31, ст.

каждому гарантируется свобода литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом» (ч.1 ст. 44);
каждый имеет право на участие в культурной жизни и пользование учреждениями культуры, на доступ к культурным ценностям» (ч.1 ст. 44);

Гарантия свободы производства и распространения массовой информации провозглашается в ст. 29: «5. Гарантируется свобода массовой информации. Цензура запрещается».

Право на информацию может быть ограничено федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороноспособности страны и безопасности государства. В этой связи в Конституции РФ особое внимание обращено на вопросы защиты государственной тайны (ст. 29): «4. Перечень сведений, составляющих государственную тайну,' определяется федеральным законом», т.е. право на доступ к информации может ограничиваться только законом.

В ст. 23 Конституции РФ среди информации о гражданах различаются личная, семейная тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. На основании судебного решения возможно ограничение права на этот вид информации.

В соответствии с *п. 1 ст. 24 Конституции РФ* сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается.

Ст. 42 Конституции РФ закрепляет право на достоверную информацию об окружающей среде.

Ст. 46 Конституции РФ гарантирует свободу литературного, художественного, научного, технического и других видов творчества, преподавания. Интеллектуальная собственность охраняется законом.

Конституция РФ защищает общество и каждого гражданина от распространения вредной, опасной информации (ст. 29):

«2. Не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства».

Каждый вправе обращаться в межгосударственные органы по защите прав и свобод человека, если исчерпаны все имеющиеся внутригосударственные средства правовой защиты (*ст. 46*), включая случаи нарушения права на информацию.

В то же время Конституция определяет, что осуществление гражданином права на информацию не должно нарушать права и свободы других лиц РФ (*ч. 3 ст. 17*).

Контрольные вопросы:

1. Дайте определение информационным правоотношениям.
2. Раскройте содержание информационного законодательства как самостоятельной отрасли права.
3. Что понимается под законодательством в области обеспечения информационной безопасности?
4. Что такое нормативный правовой акт?
5. Приведите классификацию нормативных правовых актов по юридической силе.
6. Что такое закон и каковы его основные признаки?
7. Перечислите и опишите виды подзаконных нормативных актов.
8. Приведите структуру нормативных правовых актов в области информационной безопасности.
9. Перечислите основные международные правовые акты в области информационной безопасности.
10. Перечислите основные нормативные правовые акты федерального уровня в области информационной безопасности.
11. Перечислите основные концептуальные документы в области информационной безопасности.
12. Перечислите основные подзаконные нормативные документы в области информационной безопасности.
13. Каково содержание Конституции Российской Федерации о правах и обязанностях граждан России в сфере обеспечения информационной безопасности?

ГЛАВА 4. ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРАВООТНОШЕНИЙ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Объект правоотношений в сфере обеспечения информационной безопасности

Информационная сфера или среда — сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации.

Информационная сфера как сфера правового регулирования – совокупность субъектов права, осуществляющих такую деятельность, объектов права, по отношению к которым или в связи с которыми эта деятельность осуществляется, и социальных отношений, регулируемых правом или подлежащих правовому регулированию[1].

Основным объектом правоотношений в информационной сфере является информация.

Информация (от лат. informatio, разъяснение, изложение, осведомленность) – сведения о чем-либо независимо от формы их представления.

С.И. Ожегов дает следующее определение информации: 1) сведения об окружающем мире и протекающих в нем процессах; 2) сообщения, осведомляющие о положении дел, о состоянии чего-либо[2].

В современной науке рассматриваются два подхода к понятию информации:

Объективная (первичная) информация – свойство материальных объектов и явлений (процессов) порождать многообразие состояний, которые посредством взаимодействий (фундаментальные взаимодействия) передаются другим объектам и запечатлеваются в их структуре[3].

Субъективная (семантическая, смысловая, вторичная) информация – смысловое содержание объективной информации об объектах и процессах материального мира, сформированное сознанием человека с помощью смысловых образов (слов, образов и ощущений) и зафиксированное на каком-либо материальном носителе.

При рассмотрении информации в качестве предмета правоотношений в правовой системе, предмета отношений государства, юридических и физических лиц приходится возвращаться к определению информации в

[1] Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / С.Я. Казанцев, [и др.]; под ред. С.Я. Казанцева. – М.: Издательский центр «Академия», 2005. – 240 с.

[2] Ожегов, С. И. Толковый словарь русского языка. 100 000 слов, терминов и выражений / С.И. Ожегов. - М.: Мир и Образование, 2015. - 759 с.

[3] В. М. Глушков, [и др.] Энциклопедия кибернетики. Киев, - 1975.

его исходном смысле: под информацией понимается содержание сообщений, сведений и сигналов.

Это верно постольку, поскольку при движении информации в процессе ее создания, распространения, преобразования и потребления подавляющее большинство общественных отношений возникает именно по поводу информации в форме сведений или сообщений. Такой подход к определению понятия «информация» получил название антропоцентрический[1].

В научной литературе встречается большое множество определений «информации». Следует признать, что даже достаточно полного, не говоря уж о всеобъемлющем, определения информации дать невозможно, что в каждой научно-прикладной ситуации её определение имеет свое значение и выполняет свои функции. Так, например, в философских работах развиваются представления об информации как о некой фундаментальной субстанции, стоящей в одном ряду с материей и энергией, или о том, что информационные взаимодействия – это всего лишь некие формы процессов «отражения», присущих как материальному, так и духовному миру. В естественных науках же под информацией, как правило, понимаются знания об объектах и процессах окружающего нас мира ранее получателю неизвестные.

Правовое определение информации ввел Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995 № 24-ФЗ[2] ныне утративший силу. В соответствии с ним «информация – это сведения о лицах, предметах, фактах, событиях, процессах независимо от формы их представления». В настоящее время ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3] (далее Закон «Об информации») дает следующее определение информации:

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

В соответствии со ст. 5 Закона «Об информации» информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

---

[1] Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / С.Я. Казанцев, [и др.]; под ред. С.Я. Казанцева. – М.: Издательский центр «Академия», 2005. – 240 с.

[2] Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (утратил силу) // СЗ РФ. – 1995. - № 8 ст. 609.

[3] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. -№31 (1 ч.) - ст. 3448.

При рассмотрении информации как объекта правового регулирования сферы информационной безопасности необходимо уточнить понятие и сущность *правовой информации*. Правовая информация является разновидностью информации. Ее источники: правовые нормы, институты, отрасли права, законодательство.

Существует большое количество *критериев классификации правовой информации*:

по видам источников информации (люди, документы, публикации, технические носители, продукция, технические средства обеспечения производственной деятельности);

роли информации в правовой системе (нормативная правовая, ненормативная правовая);

степени доступа к информации (открытая, ограниченного доступа);

степени официальности (официальная, неофициальная);

организационным формам представления (документальная, архивный документ, информационные ресурсы, информационные продукты) и др.

Обеспечение безопасности информации требует сохранения следующих ее свойств:

1) целостности;

2) доступности;

3) конфиденциальности.

Целостность информации заключается в ее существовании в неискаженном виде, неизменном по отношению к некоторому ее исходному состоянию.

Доступность информации — это свойство, характеризующее ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

Конфиденциальность информации — это свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.

4.2. Понятие и виды защищаемой информации

В соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006)[1] *защищаемая информация* – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

[1] Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).

Защищаемая информация имеет следующие *отличительные признаки*:

засекречивать информацию, то есть ограничивать к ней доступ, может только ее обладатель;

чем важнее для обладателя информация, тем тщательнее он ее защищает в соответствии с присвоенной ей степенью секретности;

защищаемая информация должна иметь определенную ценность и приносить пользу ее обладателю, оправдывая затрачиваемые на ее защиту силы и средства.

Появление новой защищаемой информации есть результат деятельности субъекта – обладателя информацию. После создания она как бы отчуждается от субъекта-автора, самостоятельно диктуя всем, кто с нею сталкивается, правила ее использования. Уровень защиты информации определяется установленным ее автором или обладателем грифом секретности или конфиденциальности.

Созданная один раз защищаемая информация (как и несекретная) может быть использована многократно в течение неограниченного времени сколь угодно большим количеством потребителей. Она обладает способностью не уничтожаться, не убывать со временем и даже возрастать по мере использования, то есть порождать новую информацию. Свойство возрастания информации создает объективные предпосылки для ее уязвимости.

Существует и такая особенность, как распространение информации. Для открытой информации оно имеет случайный характер, тогда как распространение защищаемой информации происходит детерминированно: заранее определяется возможное количество потребителей засекреченной информации, в соответствии с которым размножается определенное количество экземпляров соответствующего документа, которые и рассылаются заранее определенным адресатам.

Классификация защищаемой информации может осуществляться по различным основаниям. Рассмотрим наиболее распространенные: по принадлежности, степени секретности и по содержанию.

По принадлежности защищаемая информация может быть классифицирована в соответствии с тем, кто является ее обладателем:

государство и его структуры (органы) – они могут использовать сведения, составляющие государственную, служебную или коммерческую тайну, а также иные виды защищаемой информации, принадлежащей государству или ведомству;

предприятия, товарищества, акционерные общества и др. – принадлежащая им защищаемая информация обычно составляет коммерческую тайну, но в некоторых случаях они могут использовать и сведения, составляющие государственную или служебную тайну;

общественные организации – используемая ими защищаемая информация является партийной тайной, однако в некоторых случаях они могут также располагать сведениями, составляющими государственную или коммерческую тайну;

граждане – их права на тайну переписки, телефонных и иных переговоров, врачебную тайну и другие конституционные права гарантируются государством.

Классификация информации *по степени секретности* (для негосударственных структур – конфиденциальности) выглядит несколько абстрактной, однако она дает возможность ранжировать защищаемую информацию по степени ее важности. Всю информацию по степени ее секретности (конфиденциальности) можно разделить на пять уровней: особой важности (особо важная), совершенно секретная (строго конфиденциальная), секретная (конфиденциальная), для служебного пользования (не для печати, рассылается по списку), несекретная (открытая).

По *содержанию* защищаемая информация может быть разделена на политическую, экономическую, военную, разведывательную и контрразведывательную, оперативно-розыскную, научно-техническую, технологическую, деловую и коммерческую.

По категории доступа информация делится на *общедоступную информацию и информацию с ограниченным доступом* (информация ограниченного доступа) (п.3 ст.5 Закона «Об информации»).

В п. 4 ст. 8. Закона «Об информации, информационных технологиях и о защите информации»[1] имеется перечень сведений, к которым *не может быть ограничен доступ. К такой информации относятся:*

нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

сведения о состоянии окружающей среды;

сведения о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информация, накапливаемая в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

[1] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. -№31 (1 ч.) - ст. 3448.

иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

Информация с ограниченным доступом, в свою очередь, подразделяется на *сведения, составляющие государственную тайну*, и *конфиденциальную информацию.*

В ст. 2 Закона «Об информации» установлено, что такое свойство информации, как «конфиденциальность», обусловлено обязательным выполнением лицом, получившим к такой информации доступ, требования не передавать эту информацию третьим лицам без согласия ее обладателя.

Виды конфиденциальной информации установлены Указом Президента РФ № 188 от 6 марта 1997 г. «Об утверждении перечня сведений конфиденциального характера»[1], в соответствии с которым к конфиденциальной информации относятся:

персональные данные;

сведения, составляющие тайну следствия и судопроизводства;

служебная тайна;

сведения, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

коммерческая тайна;

сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них и некоторые другие;

сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве»[2].

В настоящее время единой и четкой классификации конфиденциальной информации в литературе не существует, тем не менее, в соответствии с действующими нормативными актами названо свыше 20 разновидностей конфиденциальной информации.

[1] Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. — 1997.-№ 10-ст. 1127.

[2] Федеральный закон от 2 октября 2007 г. № 229-ФЗ "Об исполнительном производстве" // Собрание законодательства Российской Федерации от 8 октября 2007 г. № 41 ст. 4849.

4.3. Правовое обеспечение защиты критической информационной инфраструктуры

Основным документом, регламентирующим защиту объектов критической информационной инфраструктуры, является Федеральный закон от 26.07.2017 № 187-ФЗ[1] (вступил в силу с 1 января 2018 года), который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Под критической информационной инфраструктурой (КИИ) понимаются объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Объекты КИИ – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Кроме того, вводится понятие значимого объекта КИИ - объекта КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ;

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Ст. 4) принципами обеспечения безопасности КИИ являются:

законность;

непрерывность и комплексность обеспечения безопасности КИИ, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов КИИ;

приоритет предотвращения компьютерных атак.

В данном случае выделение предотвращения компьютерных атак как обособленного принципа обусловлено особенностями объекта защиты (построения объектов КИИ на базе автоматизированных систем).

В соответствие со ст. 11 рассматриваемого федерального закона требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры.

Обеспечения безопасности КИИ включает в себя (укрупненно) следующие этапы:

определение, является ли информационная система объектом КИИ;

[1] О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26 июля 2017 г. №187-ФЗ // Собр. законодательства Рос. Федерации. - 2017. - № 31. - Части I-II. - Ст. 4736.

определение категории значимости объекта КИИ;

реализация мероприятий по защите информации (включая контроль эффективности принятых мероприятий по защите КИИ);

госконтроль в области обеспечения безопасности значимых объектов КИИ.

Президент Российской Федерации определяет:

основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры;

федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

порядок создания и задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Правительство Российской Федерации устанавливает:

показатели критериев значимости объектов критической информационной инфраструктуры и их значения, а также порядок и сроки осуществления их категорирования;

порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;

утверждает порядок ведения реестра значимых объектов критической информационной инфраструктуры и ведет данный реестр;

утверждает форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;

устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (требования по

обеспечению безопасности информационно-телекоммуникационных сетей, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов критической информационной инфраструктуры, устанавливаются по согласованию с федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи), а также требования к созданию систем безопасности таких объектов и обеспечению их функционирования (в банковской сфере и в иных сферах финансового рынка устанавливает указанные требования по согласованию с Центральным банком Российской Федерации);

осуществляет государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также утверждает форму акта проверки, составляемого по итогам проведения указанного контроля.

Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;

создает национальный координационный центр по компьютерным инцидентам и утверждает положение о нем;

координирует деятельность субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

организует и проводит оценку безопасности критической информационной инфраструктуры;

определяет перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и порядок ее представления;

утверждает порядок информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры (в банковской

сфере и в иных сферах финансового рынка утверждает указанный порядок по согласованию с Центральным банком Российской Федерации);

утверждает порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, а также порядок получения субъектами критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения;

организует установку на значимых объектах критической информационной инфраструктуры и в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

утверждает порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (в банковской сфере и в иных сферах финансового рынка утверждает указанные порядок и технические условия по согласованию с Центральным банком Российской Федерации).

Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи, утверждает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры.

Отнесение объекта к КИИ осуществляется в соответствие с Федеральным законом от 26.07.2017 № 187-ФЗ (исходя из понятия КИИ).

Определение категории значимости объекта КИИ регламентирует постановление Правительства Российской федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»[1].

Категорирование осуществляется субъектами критической информационной инфраструктуры в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры.

Постановление Правительства Российской федерации от 8 февраля 2018 г. № 127 определяет:

правила категорирования объектов критической информационной инфраструктуры Российской Федерации;

перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений.

Устанавливаются 3 категории значимости. Самая высокая категория – первая, самая низкая – третья.

Мероприятия по защите информации определяются в соответствие с Приказом ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [2] (далее – Требования) и Приказом ФСТЭК России от 26 марта 2019 г. № 60 «О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239»[3].

Требования разработаны в соответствии с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и направлены на обеспечение устойчивого функционирования значимых объектов КИИ Российской Федерации при проведении в отношении них компьютерных атак.

---

[1] Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : постановление Правительства РФ от 08 февраля 2018 г. № 127 (ред. от 13 апреля 2019 г.) // Собр. законодательства Рос. Федерации. - 2018. - № 8. - Ст. 1204.

[2] Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России от 25 декабря 2017 г. № 239 // http://fstec.ru.

[3] О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 : Приказ ФСТЭК России от 26 марта 2019 г. № 60 // http://fstec.ru.

Государственный контроль в области обеспечения безопасности значимых объектов КИИ осуществляется на основании постановления Правительства РФ № 162 от 17.02.2018 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»[1], которое устанавливает порядок осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ Российской Федерации (ФСТЭК России), и его территориальными органами мероприятий по государственному контролю в области обеспечения безопасности значимых объектов КИИ Российской Федерации.

Контрольные вопросы:

1. Что понимается под информационной сферой как сферой правового регулирования?
2. Приведите известные Вам понятия «информация».
3. Каковы особенности правовой информации?
4. Приведите известные Вам критерии классификации правовой информации.
5. Что означает термин «целостность информации»?
6. Что означает термин «доступность информации»?
7. Что означает термин «конфиденциальность информации»?
8. Что такое защищаемая информация и каковы ее отличительные признаки?
9. Перечислите известные Вам критерии классификации защищаемой информации.
10. К какой информации не может быть ограничен доступ?
11. Какие сведения относятся к информации с ограниченным доступом?
12. Перечислите принципы обеспечения безопасности КИИ.
13. Перечислите этапы обеспечения безопасности КИИ.
14. Перечислите функции Президента Российской Федерации в области обеспечения безопасности КИИ.

[1] Постановление Правительства РФ от 17 февраля 2018 г. № 162 “Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации”

ГЛАВА 5. ГОСУДАРСТВЕННАЯ ТАЙНА КАК ОСОБЫЙ ВИД ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

5.1. Понятие и сущность государственной тайны

Понятие *«государственная тайна»* занимает одно из ключевых положений в системе обеспечения безопасности любого государства. Определение этого понятия дано в ст. 2 Закона РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» (далее Закон «О государственной тайне»)[1]: «*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».

В ст. 5 указанного закона приведен *перечень сведений, составляющих государственную тайну* (указаны лишь разделы): в военной области; о внешнеполитической и внешнеэкономической деятельности; в области экономики, науки и техники; в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Какие сведения могут быть отнесены к государственной тайне, определено в Указе Президента РФ от 30 ноября 1995 г. № 1203[2]. Данным Указом существенно конкретизирован перечень групп сведений, составляющих государственную тайну, и увеличен до 119. Также данный документ определяет государственные органы и организации, которые наделены полномочиями по распоряжению сведениями, отнесенными к государственной тайне

Закон и Перечень содержат только категории сведений, составляющих государственную тайну, а не сами сведения, которые являются государственной тайной. Соответственно, ни закон, ни Перечень не устанавливают степени секретности сведений, т.е. не засекречивают их.

В соответствии со статьей 7 Закона «О государственной тайне» *не подлежат засекречиванию и подлежат обязательному рассекречиванию без ограничения хронологических рамок документы, содержащие сведения*:

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

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

---

[1]Закон Российской Федерации «О государственной тайне» от 21.07.1993 № 5485-1 (ред. от 18 июля 2009) // Собрание законодательства РФ. - 1997. - № 2

[2] Указ Президента РФ от 30 ноября 1995 года № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» // СЗ РФ. 1995. - № 49 - ст. 4775.

о привилегиях, компенсациях и льготах, 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 Российской Федерации;

о состоянии здоровья высших должностных лиц Российской Федерации;

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

Положения данной статьи также закрепляет, что в случае засекречивания перечисленных выше сведений должностные лица, принявшие такое решение, могут быть привлечены к юридической ответственности (уголовной, административной или дисциплинарной ответственности). Таким образом, если гражданину было отказано в ознакомлении с информацией, которая не подлежит засекречиванию, то он имеет право обжаловать подобные действия должностных лиц в вышестоящей инстанции или требовать ее предоставления через судебные органы.

5.2. Правовое обеспечение защиты государственной тайны

Одним из наиболее эффективных способов защиты информации является ее засекречивание. Под з*асекречиванием сведений и их носителей* следует понимать ограничения на их распространение и на доступ к их носителям.

Основными *принципами* отнесения сведений к государственной тайне и их засекречивания являются принципы законности, обоснованности и своевременности.

Согласно Перечню должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне, утвержденным Распоряжением Президента РФ от 16.04.2005 № 151-рп[1], в него входят:

Руководитель Администрации Президента Российской Федерации;

Первый заместитель Председателя Правительства Российской Федерации – Министр финансов Российской Федерации;

Заместитель Председателя Правительства Российской Федерации – Руководитель Аппарата Правительства Российской Федерации;

Министр внутренних дел Российской Федерации;

[1] Распоряжение Президента РФ от 16 апреля 2005 г. № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» // СЗ РФ. 2005. - № 17 - ст. 1547.

Министр Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;

Министр иностранных дел Российской Федерации;

Министр обороны Российской Федерации;

Министр юстиции Российской Федерации;

Министр здравоохранения Российской Федерации;

Министр науки и высшего образования Российской Федерации;

Министр природных ресурсов и экологии Российской Федерации;

Министр промышленности и торговли Российской Федерации;

Министр сельского хозяйства Российской Федерации;

Министр транспорта Российской Федерации;

Министр цифрового развития, связи и массовых коммуникаций Российской Федерации;

Министр строительства и жилищно-коммунального хозяйства Российской Федерации;

Министр экономического развития Российской Федерации;

Министр энергетики Российской Федерации;

Председатель Банка России;

Директор ГФС России;

Директор СВР России;

Директор ФСБ России;

Директор Росгвардии – главнокомандующий войсками национальной гвардии Российской Федерации;

Директор ФСО России;

Начальник ГУСПа;

Директор ФСТЭК России;

Руководитель ФТС России;

Генеральный директор Государственной корпорации по атомной энергии «Росатом»;

Генеральный директор Государственной корпорации по космической деятельности «Роскосмос»;

Директор Росфинмониторинга;

Руководитель Роспотребнадзора;

Руководитель Росрезерва.

В ст. 8 Закона «О государственной тайне» установлены степени секретности сведений и грифы секретности носителей этих сведений. *Степень секретности* сведений, составляющих государственную тайну, соответствует степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации в случае распространения этих сведений. Законом «О государственной тайне»[1] установлены *три степени секретности:*

[1] Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» // СЗ РФ. 1997. - № 41 - ст. 8220-8235.

«особой важности»;
«совершенно секретно»;
«секретно».

В соответствии с Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности (утв. Постановлением Правительства РФ от 4 сентября 1995 г. № 870 [1]) к сведениям *особой важности* следует относить сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей; к *совершенно секретным* сведениям - сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации; к *секретным* сведениям - все иные сведения из числа сведений, составляющих государственную тайну.

Проект перечня разрабатывает специально созданная *экспертная комиссия*. В ее состав включаются компетентные специалисты, работающие со сведениями, составляющими государственную тайну. Для определения этих сведений специалисты анализируют деятельность органов государственной власти, предприятий, учреждений и организаций. Собственники информации готовят обоснование необходимости отнесения сведений к государственной тайне с указанием соответствующей степени секретности. В случае, если сведения находятся в распоряжении нескольких органов государственной власти, степень секретности устанавливается по взаимному согласованию между ними.

Проект перечня утверждается руководителем органа государственной власти. Для координации работ утвержденные перечни направляются в Межведомственную комиссию по защите государственной тайны.

Каждые 5 лет перечни подлежат пересмотру. Возможен пересмотр в случае необходимости (например, в случае изменения международной обстановки). Пересмотр перечней осуществляется в том же порядке, что и их разработка.

Порядок засекречивания сведений и их носителей установлен ст.11 Закона «О государственной тайне». Перечень сведений, подлежащих засекречиванию, является *основанием* для засекречивания сведений. На носителях, содержащих сведения, составляющие государственную тайну, проставляется соответствующий гриф секретности.

В случае, если на носителе невозможно нанести указанные реквизиты, они отмечаются в сопроводительной документации на этот носитель.

---

[1]Постановление Правительства РФ от 4 сентября 1995 г. № 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" // СЗ РФ. 1995. № 37. Ст. 3619.

Порядок рассекречивания сведений предусмотрен ст. 13 Закона «О государственной тайне»[1]. *Рассекречивание сведений и их носителей* - снятие ранее введенных ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям. Закон «О государственной тайне» выделяет два о*снования* рассекречивания сведений:

взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну;

изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной.

Общий срок засекречивания сведений, составляющих государственную тайну, не может быть более *30 лет*. По решению межведомственной комиссии по защите государственной тайны срок может быть продлен.

Ограничение доступа в государственной тайне

Под допуском к государственной тайне в соответствии с Законом «О государственной тайне» следует понимать процедуру оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений. Допуск осуществляется в добровольном порядке (ст. 21).

Вопросы, связанные с допуском к государственной тайне, регламентированы Инструкцией о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне, утвержденной Постановлением Правительства РФ от 6 февраля 2010 г. № 63[2].

Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне регламентирован Постановлением Правительства РФ от 22 августа 1998 г. № 1003 "Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне"[3].

---

[1] Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» // СЗ РФ. 1997. - № 41 - ст. 8220-8235.

[2]Постановление Правительства РФ от 06.02.2010 № 63 (ред. от 29.12.2016) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне". Собрание законодательства РФ, 15.02.2010, № 7, ст. 762.

[3]Постановление Правительства РФ от 22.08.1998 № 1003 "Об утверждении положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне" // Собрание законодательства РФ", 31.08.1998, № 35, ст. 4407

Наличие д*опуска* должностных лиц и граждан к государственной тайне выражено в следующем:

лицо принимает на себя обязательства перед государством по нераспространению доверенных ему сведений;

лицо дает согласие на частичные, временные ограничения их прав;

необходимо письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

определяются виды, размеры и порядок предоставления социальных гарантий;

лицо должно ознакомиться с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение.

Решение о допуске оформляемого лица к сведениям, составляющим государственную тайну, принимает руководитель органа государственной власти, предприятия, учреждения или организации.

Законом «О государственной тайне» предусмотрены две социальные гарантий для лиц, допущенных к государственной тайне на постоянной основе, а именно:

процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий.

Постановлением Правительства РФ от 18 сентября 2006 г. № 573[1] утверждены Правила выплаты ежемесячных процентных надбавок к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе, и сотрудников структурных подразделений по защите государственной тайны.

Законом «О государственной тайне» установлены *три формы допуска:*

1-я форма допуска предполагает доступ *к* сведениям особой важности, совершенно секретным и секретным сведениям;

2-я форма допуска - *доступ к* совершенно секретным и секретным сведениям;

3-я форма допуска - *доступ к* секретным сведениям.

При оформлении той или иной формы допуска в трудовом договоре отражаются обязательства гражданина по соблюдению требований законодательства о государственной тайне.

---

[1] Постановление Правительства РФ от 6 июня 2008 г. № 440 «О внесении изменения в Постановление Правительства Российской Федерации от 18 сентября 2006 г. № 573» // СЗ РФ. 2008. - № 23 - ст. 2727.

Основаниями для отказа гражданину в допуске к государственной тайне могут являться:

а) признание гражданина судом недееспособным, ограниченно дееспособным или рецидивистом, нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у гражданина неснятой судимости за эти преступления;

б) наличие у гражданина медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Приказом Министерства здравоохранения и социального развития Российской Федерации (Минздравсоцразвития России) от 26 августа 2011 г. №989н г. Москва «Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну»[1];

в) постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными гражданами документов для выезда на постоянное место жительства в другие государства;

г) выявление в результате проведения проверочных мероприятий действий гражданина, создающих угрозу безопасности Российской Федерации;

д) уклонение гражданина от проверочных мероприятий и (или) сообщение заведомо ложных анкетных данных.

Прекращение допуска осуществляется по решению должностного лица, принявшего решение о его допуске к государственной тайне. Закон о «Государственной тайне» выделяет 3 случая:

расторжения трудового договора (контракта) в связи с проведением организационных и (или) штатных мероприятий;

однократного нарушения обязательств, связанных с защитой государственной тайны;

при возникновении обстоятельств, являющихся основанием для отказа гражданину в допуске к государственной тайне.

Гражданин имеет право обжаловать решение о прекращении допуска к государственной тайне в вышестоящей организации или в суде.

Прекращение допуска к государственной тайне не дает право гражданину разглашать доверенные ему государством сведения.

---

[1] Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских противопоказаний для работы с использований сведений, составляющих государственную тайну : приказ Минздравсоцразвития РФ от 26.08.2011 № 989н (Зарегистрировано в Минюсте РФ 11.10.2011 № 22016) // Российская газета. 2011. № 234.

Руководители организаций несут персональную ответственность за подбор граждан, допускаемых к государственной тайне.

Контрольные вопросы:

1. Что понимается под термином «государственная тайна»?
2. В каких нормативных правовых документах содержатся категории сведений, составляющих государственную тайну?
3. Какие сведения не подлежат засекречиванию?
4. Что такое засекречивание сведений и их носителей?
5. Каковы принципы засекречивания информации?
6. Перечислите должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.
7. Какие степени секретности установлены Законом «О государственной тайне»?
8. Что такое защищаемая информация и каковы ее отличительные признаки?
9. Каковы правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?
10. Что такое рассекречивание информации и их носителей?
11. Что такое допуск к государственной тайне?
12. Что для гражданина предусматривает допуск к государственной тайне?
13. Перечислите социальные гарантии, установленные для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе.
14. Перечислите основания для отказа гражданину в допуске государственной тайне.
15. Перечислите основания прекращения допуска к государственной тайне.

ГЛАВА 6. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

6.1. Персональные данные как вид защищаемой информации

Система источников законодательства
в области персональных данных

Законодательство о персональных данных является сравнительно молодым, но динамично развивающимся. Первые упоминания о персональных данных в российском законодательстве появились в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» [1] . Однако детальное регулирование было осуществлено лишь с принятием в 2006 г. Закона о персональных данных, который не только был основан на положениях Конвенции 1981 г., ратифицированной Россией в 2005 г.[2], но и заимствовал многие нормы Директивы 1995 г.[3] (особенно в массивном пакете поправок, принятых в 2011 г.). Регулирование отношений, связанных с обработкой персональных данных, осуществляется исключительно на уровне нормативных правовых актов федерального уровня. Это обусловлено направленностью законодательства о персональных данных на защиту конституционного права на неприкосновенность частной жизни, личную и семейную тайну, а также иных прав и свобод, связанных с обработкой персональных данных. При этом в соответствии с подп. «в» п. 1 ст. 71 Конституции РФ [4] регулирование и защита прав и свобод человека и гражданина как высших демократических ценностей отнесены к исключительному ведению Российской Федерации.

Закон о персональных данных является базовым законодательным актом, регулирующим отношения, связанные с обработкой персональных данных, и определяет принципы, условия и правила обработки персональных данных. Иные федеральные законы могут конкретизировать случаи и особенности обработки отдельных категорий персональных данных, но не могут устанавливать иные принципы обработки

---

[1] Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (утратил силу)// СЗ РФ. – 1995. - № 8 ст. 609.

[2] Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных»//Москва, Кремль;19 декабря 2005 г.№ 160-ФЗ

[3] Директива 95/46/ЕС Европейского Парламента и Совета от 24 октября 1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (Принята в г. Люксембурге 24.10.1995, с изм. и доп. от 29.09.2003 г.).— Официальный Журнал Европейского Союза.— № L 281.— 23.11.1995.— p. 31.

[4] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)// Собрание законодательства РФ, 04.08.2014, № 31, ст.

персональных данных или давать дефиниции ключевых терминов. Примером такого федерального закона служит Трудовой кодекс РФ, который содержит специальную главу (гл. 14), посвященную особенностям защиты персональных данных работников. Другим примером подобного акта является Федеральный закон от 7 июня 2013 г. № 108-ФЗ «О подготовке и проведении в Российской Федерации чемпионата мира по футболу ИБЛ 2018 года, Кубка конфедераций ИБЛ 2017 года и внесении изменений в отдельные законодательные акты Российской Федерации»[1], который содержит специальную статью (ст. 23.1), посвященную особенностям обработки персональных данных граждан Российской Федерации в процессе подготовки и проведения указанных мероприятий.

Среди важных документов, формально не являющихся нормативными правовыми актами, но оказывающими немалое влияние на правоприменительную практику в сфере законодательства о персональных данных, следует отметить разъяснения Минкомсвязи России, которое является федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере обработки персональных данных, и уполномочено на дачу разъяснений по данным вопросам . Кроме них также следует упомянуть комментарии и информацию Роскомнадзора, которые хотя и не являются официальными актами толкования законодательства, но могут оказывать существенное влияние на практику в силу убедительности содержащихся в них аргументов либо в силу статуса лица, которое их предоставило.

Согласно ч. 3 ст. 4 порядок обработки персональных данных, осуществляемой без использования средств автоматизации, может устанавливаться федеральными законами и иными нормативными правовыми актами Российской Федерации. В настоящее время одним из таких актов является Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства РФ от 15 сентября 2008 г. № 687[2].

К важнейшим международным договорам, имеющим отношение к защите персональных данных, следует отнести Международный пакт от 16 декабря 1966 г. «О гражданских и политических правах»[3], ст. 17 которого предусматривает, что «никто не может подвергаться произвольному или

---

[1] Федеральный закон от 07.06.2013 № 108-ФЗ (ред. от 29.12.2017) «О под-готовке и проведении в Российской Федерации чемпионата мира по футболу FIFA 2018 года, Кубка конфедераций FIFA 2017 года и внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. - 10.06.2013. - № 23. - ст. 2866.

[2] Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: постановление Правительства РФ от 15.09.2008 № 687 // Российская газета. 2008. 24 сентября.

[3] Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) // Ведомости Верховного Совета СССР. - 1976 г. - №17(1831). - Ст. 291.

незаконному вмешательству в его личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на его честь и репутацию». Кроме того, следует отметить положение ст. 8 Конвенции о защите прав человека и основных свобод 1950 г.[1], по которому «каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции».

Основным международным договором в сфере персональных данных с участием России является Конвенция 1981 г.[2] Данный документ закрепил фундаментальные принципы обработки персональных данных, которые были имплементированы в Закон о персональных данных. Следует отметить, что положения Конвенции не устанавливают непосредственно права и обязанности участников отношений, связанных с обработкой персональных данных, а создают обязательства для государства по их имплементации в национальное право (ст. 4 (1)). Как следствие, положения данной Конвенции не действуют в России непосредственно. Кроме того, важно подчеркнуть, что Конвенция 1981 г. допускает возможность присоединяющейся стороны сделать заявление об отдельных изъятиях в сфере ее применения. Российская Федерация воспользовалась этим положением, заявив, что не будет применять Конвенцию к персональным данным, обрабатываемым физическими лицами исключительно для личных и семейных нужд, а также к данным, отнесенным к государственной тайне. Кроме того, Российская Федерация прямо указала на то, что сохраняет за собой возможность устанавливать ограничения прав субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

Рассматривая систему источников законодательства в области персональных данных, нельзя не упомянуть акты, которые хотя и не содержат юридически обязательных норм, но фактически оказывают серьезное влияние на регулирование отношений, связанных с реализацией оператором организационных и технических мер защиты персональных данных. К таким актам относятся национальные стандарты, каждый из которых - это документ по стандартизации, который разработан участником или участниками работ по стандартизации, по результатам экспертизы в техническом комитете по стандартизации или проектном техническом комитете по стандартизации, утвержден федеральным органом исполнительной власти в сфере стандартизации, и в нем для всеобщего применения устанавливаются общие характеристики объекта стандартизации, а также правила и общие принципы, применяемые в

[1] Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21 сентября 1970 г., 20 декабря 1971 г., 1 января 1990 г., 6 ноября 1990 г., 11 мая 1994 г.) // Бюллетень международных договоров. - март 2001 г. - №3.

[2] Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 г.

отношении объекта стандартизации (п. 5 ст. 2 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации»[1]). К числу стандартов, релевантных проблематике защиты персональных данных, можно отнести следующие:

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

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

ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;

ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования;

ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 г. № 1340-ст);

ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст);

ГОСТ Р ИСО/МЭК 27002-2012. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. № 423-ст);

ГОСТ Р ИСО/МЭК 27003-2012. Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 812-ст);

ГОСТ Р ИСО/МЭК 27004-2011. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 681-ст);

ГОСТ Р ИСО/МЭК 27005-2010. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска

[1] Федеральный закон "О стандартизации в Российской Федерации" от 29.06.2015 № 162-ФЗ

информационной безопасности (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст);

ГОСТ Р ИСО/МЭК 27006-2008. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 524-ст).

Понятие и категории персональных данных

Изначально в Указе Президента РФ от 06.03.1997 № 188 [1], *персональные данные* определяются как «сведения о фактах, событиях и обстоятельствах частной жизни, позволяющие идентифицировать субъекта», а позже в ФЗ №152 [2] под такими данными стала пониматься «любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)» (ст. 3). Исходя из определения, закрепленного Указе Президента РФ от 06.03.1997 № 188 [3], персональными данными являются только такие сведения, которые, относятся к частной жизни гражданина и носят идентифицирующий его характер. А по смыслу второго определения данного в ФЗ №152 к ним относится любая информация, даже та, которая не имеет непосредственного отношения к определенному лицу. В данном случае, указания на характер сведений, представляющих собой персональные данные, вообще отсутствуют. Приведенное определение практически дословно воспроизводит определение, закрепленное в Директиве № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных»[4].

Рассмотрение вопроса о месте персональных данных в системе информации ограниченного доступа требует обращения еще к одному нормативному правовому акту - Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»[5] (далее – Закон об информации). Данный закон определяет

[1] Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 // Собрание законодательства РФ. - 1997. - № 10. - Ст. 1127.

[2] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.

[3] Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 // Собрание законодательства РФ. - 1997. - № 10. - Ст. 1127.

[4] Директива Европейского парламента и Совета Европейского союза от 24 октября 1995 года № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (в редакции Регламента Европейского парламента и Совета Европейского союза от 29 сентября 2003 г. № 1882/2003) [Электронный ресурс] - Режим доступа. - URL: http://online.zakon.kz/Document/ (дата обращения: 11.09.2019).

[5] Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.

информацию как «сведения (сообщения, данные) независимо от формы их представления» (п. 1 ст. 2).

Закон об информации относит персональные данные к информации ограниченного доступа. В п. 9 статьи 9 «Ограничение доступа к информации» содержится отсылочная норма к специальному законодательству в отношении персональных данных.

На основании анализа законодательства, следует полагать, что не все персональные данные охраняются режимом конфиденциальности. Некоторые данные относящиеся к категории персональных подлежат опубликованию в открытом доступе в соответствии с федеральными законами. К таким следует отнести, например, персональные данные кандидатов в депутаты, которые могут быть обнародованы по решению субъекта персональных данных, для размещения профессиональной энциклопедии.

Законодательство определяет следующие *категории персональных данных:* общедоступные ПДн, специальные категории ПДн, биометрические ПДн и иные.

Общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Такие данные могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн. Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

К *специальным категориям* относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [1]. Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-

[1] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.

розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством. Исходя из определения биометрических ПДн, к ним относятся фотографии и видеоизображения субъектов ПДн. Это подтверждают и представители регуляторов, в частности Федеральной службы по техническому и экспортному контролю. Фотографии субъектов ПДн могут обрабатываться в пропускных системах и системах контроля доступа, видеоизображения – в системах видеонаблюдения и т.п.

Требования к обеспечению защиты персональных данных

Основные требования к обеспечению защиты персональных данных установлены ФЗ №152 [1] и принятыми в его исполнение подзаконными нормативными правовыми актами. Эти требования обращены прежде всего к *операторам персональных данных*, к которым согласно ФЗ № 152 относятся государственные и муниципальные органы, юридические или физические лица, самостоятельно или совместно с другими лицами организующие / осуществляющие обработку персональных данных, а также определяющие цели их обработки, состав данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Типичными примерами операторов персональных данных являются организации, которые осуществляют обработку данных своих работников (и) или клиентов - физических лиц; лица, которые осуществляют сбор и анализ общедоступных данных в сети Интернет; государственные органы и учреждения, которые обрабатывают персональные данные граждан в процессе предоставления государственных услуг; онлайн-сервисы, которые предусматривают регистрацию пользователей и (или) собирают данные о них в процессе использования такого сервиса.

В настоящее время под *обработкой персональных данных* понимается любое действие (операция), совершаемое с персональными данными, как с использованием средств автоматизации, так и без них. К таковым относятся, в частности, сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. К обработке персональных данных в полной мере можно отнести любое действие, носящее волевой характер и сопряженное с воздействием на данные в период их жизненного цикла: обычное хранение персональных данных на жестком диске компьютерного устройства; использование компьютерных алгоритмов по глубинному анализу данных. Под *автоматизированной обработкой* понимается любая обработка персональных данных,

[1] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.

осуществляемая с использованием вычислительных средств. Иными словами, в случае, если производится обработка персональных данных, существующих в цифровой форме, то она всегда имеет автоматизированный характер.

Согласие субъекта персональных данных является единственным универсальным легитимирующим основанием для любого сбора, использования или иных видов обработки персональных данных. Все остальные основания для обработки персональных данных в отсутствие согласия их субъекта предполагают наличие либо специальной цели обработки, либо специального субъекта на стороне оператора, либо совокупности указанных факторов.

Такое согласие должно быть:

1) конкретным, т.е. явно выраженным и определенным. Факт дачи согласия не должен быть предметом домыслов, а должен следовать из конкретных действий субъекта, свидетельствующих об этом. Молчание или бездействие субъекта персональных данных, даже если такое поведение в соответствии с политикой конфиденциальности оператора будет признаваться согласием, не будет удовлетворять указанному требованию. Аналогичным образом действия субъекта персональных данных по использованию устройства или интернет-сервиса с применением настроек конфиденциальности «по умолчанию» в отсутствие каких-либо свидетельств их изменения пользователем также не удовлетворяют указанному требованию;

2) информированным, т.е. даче субъектом согласия должно предшествовать предоставление ему всей необходимой и достоверной информации о целях обработки, обрабатываемых данных, операторе и иных лицах, которые будут осуществлять обработку его персональных данных, сроки обработки и все иные релевантные параметры обработки персональных данных. Предоставляемая оператором информация должна позволять субъекту получить ответы на вопросы о том, кто, зачем, какие данные, каким образом и в течение какого срока будет обрабатывать. При этом не будет лишним предоставление расшифровки основных терминов, которые используются в соответствующем документе (форма согласия, договор), в противном случае есть риск непризнания данного согласия соответствующим указанному требованию;

3) сознательным, т.е. обдуманным и осмысленным. Соответствующая информация должна быть воспринята субъектом персональных данных и отражать его действительные намерения. Вынужденный характер дачи согласия ставит под сомнение его соответствие указанному требованию.

По общему правилу согласие на обработку персональных данных может быть дано в любой форме, позволяющей подтвердить факт его получения, если только специальная форма дачи согласия прямо не предусмотрена законом. При этом равнозначным содержащему

собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом электронной подписью (ч. 4 ст.9).

Требования к обработке персональных данных вытекают практически из каждой статьи ФЗ № 152[1], но есть статьи, непосредственно обращенные к операторам персональных данных. Это ст. 18 «Обязанности оператора при сборе персональных данных», ст. 18.1 «Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом», ст. 19 «Меры по обеспечению безопасности персональных данных при их обработке». Оператор обязан принимать меры, необходимые и достаточные для выполнения установленных обязанностей. При этом оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для их обеспечения.

Рассмотрим данные положения более подробно.

Статья 18. Обязанности оператора при сборе персональных данных

Возложенные на оператора обязанности можно разделить на два вида: информационного характера (ч. ч. 1 - 4 ст. 18) и организационно-технического характера (ч. 5 ст. 18).

Обязанности информационного характера:

обязанность оператора предоставить субъекту персональных данных информацию, указанную в ч. 7 ст. 14 ФЗ №152 (данная обязанность возникает только при наличии на то соответствующего волеизъявления со стороны субъекта персональных данных);

обязанность по разъяснению субъекту персональных данных последствий отказа от предоставления таких данных. Эта обязанность способствует обеспечению возможности принятия субъектом информированного решения о предоставлении своих данных. Одним из возможных последствий отказа от предоставления персональных данных является отказ оператора от совершения ожидаемого от него действия, которое не может быть осуществлено в отсутствие таких данных, либо в силу существа отношений, либо в силу закона (предоставление услуги, доступ в определенное помещение или транспортное средство, возможность въезда в страну и т.п.).

обязанность предоставления субъекту, в случае если информация получена не от самого субъекта, содержащуюся информацию, в частности идентифицировать себя, пользователей данных, источник получения данных и цели обработки этих данных. Возложение такой обязанности на оператора имеет своей целью обеспечение еще большей прозрачности процессов перехода персональных данных от одного оператора к другому.

[1] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.

В идеале ее выполнение может позволить субъекту персональных данных отследить факт нарушения первоначальным оператором условий данного ему согласия на обработку персональных данных или факт их обработки новым оператором без достаточных оснований. В отличие от информационной обязанности оператора по предоставлению информации субъекту при сборе данных (ч. 1 настоящей статьи) в рассматриваемом случае закон не обязывает субъекта требовать предоставления ему такой информации, предполагается безусловная обязанность ее выполнения оператором.

Обязанности организационно-технического характера:

ч. 5 ст.18 ФЗ №152 [1] закрепила обязанность оператора обеспечивать локализацию отдельных процессов обработки персональных данных, собираемых у российских граждан. Положения этой части вступили в силу 1 сентября 2015 г. и не имеют аналогов в зарубежных правопорядках, в связи с чем вопросы их толкования и соотношения с положениями о трансграничной передаче данных приобретают особую актуальность. Немаловажную роль в этом играет и возможность блокировки онлайн-ресурса оператора, который обрабатывает персональные данные граждан Российской Федерации с нарушением требований локализации в соответствии с положениями ст. 15.5 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

Следует отметить, что данная норма содержит перечень мер, которые должен принять оператор персональных данных в целях соблюдения требований ФЗ №152. Этот перечень мер носит ориентировочный характер, окончательное решение относительно таких мер принимает сам оператор по своему усмотрению, за исключением случаев, когда закон обязывает оператора принять конкретные меры.

В частности, перечень мер, которые должны принимать операторы, являющиеся государственными и муниципальными органами, дан в соответствии с ч. 3 ст.18.1 в Постановлении Правительства РФ от 21 марта 2012 г. № 211 [2]. Данный нормативный правовой акт содержит перечень локальных актов, которые должны приниматься государственными или муниципальными органами, в который входят:

1) правила обработки персональных данных, определяющие для каждой цели обработки таких данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные

[1] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.

[2] Постановлении Правительства РФ от 21 марта 2012 г. № 211// СЗ РФ. 2012. № 45 ст. 6257.

которых обрабатываются, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований;

2) правила рассмотрения запросов субъектов персональных данных или их представителей;

3) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;

4) правила работы с обезличенными данными в случае обезличивания персональных данных;

5) перечень информационных систем персональных данных. В таком документе целесообразно указать назначение системы, составляющей основную цель обработки персональных данных в ней (например, автоматизация процессов кадрового учета или процессов расчета заработной платы), категории и объем персональных данных в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119[1];

6) перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

7) перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае необходимости обезличивания персональных данных;

8) перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

9) должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе;

10) типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных

[1] Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // Собрание законодательства РФ.2012. № 45. ст. 6257.

данных, ставших известными ему в связи с исполнением должностных обязанностей;

11) типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

12) порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных.

В ст. 19 ФЗ №152[1] определены меры по обеспечению безопасности персональных данных при их обработке вне зависимости от установленного оператором режима конфиденциальности, а скорее исходя из самостоятельного режима конфиденциальности персональных данных.

Меры, указанные в данной статье, могут относиться к одной из трех групп:

1) правовые (подготовка и принятие соответствующих локальных нормативных актов);

2) организационные (назначение ответственных лиц, обучение работников, непосредственно вовлеченных в процесс обработки персональных данных, правилам информационной безопасности и т.п.);

3) технические (набор мер, направленных как на уменьшение вероятности реализации угроз информационной безопасности вследствие уязвимости информационной системы, так и на минимизацию потерь при реализации таких угроз).

Для выполнения обязанности по определению угроз безопасности персональных данных необходимо разработать документ «Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных». При этом целесообразно руководствоваться следующими документами ФСТЭК:

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК 14 февраля 2008 г.[2];

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК 15 февраля 2008 г.[3]

---

[1] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.

[2] «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» // Утверждена Заместителем директора ФСТЭК России, 15 февраля 2008 г.

[3] «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» // Утверждена Заместителем директора ФСТЭК России, 15 февраля 2008 г.

Перечень организационных и технических мер в соответствии с уровнями защищенности персональных данных, установленными Правительством РФ, предусмотрен в следующих актах:
Приказ ФСБ России от 10 июля 2014 г. № 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 ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Контроль и надзор за соблюдением установленных законодательством мер по защите персональных данных.

В свою очередь, государство в лице уполномоченных органов осуществляет *контроль и надзор за соблюдением установленных законодательством мер.* ФЗ № 152[1] содержит самостоятельную главу, посвященную государственному контролю и надзору за обработкой персональных данных, в которой имеется только одна статья, посвященная этой теме - ст. 23. Согласно ей, уполномоченный орган по защите прав субъектов персональных данных обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям ФЗ № 152 и принятых в соответствии с ним нормативных правовых актов. В настоящее время функции контроля за выполнением операторами установленных требований возложены на Роскомнадзор. В соответствии с ч. 1.1 ст. 23 ФЗ № 152 порядок организации и проведения проверок юридических лиц и индивидуальных предпринимателей, являющихся операторами обработки персональных данных, уполномоченным органом по защите прав субъектов персональных данных, а порядок организации и осуществления государственного контроля и надзора за их обработкой иными лицами, являющимися операторами, устанавливается Правительством Российской Федерации.

При исполнении контрольных функций Роскомнадзор действует в соответствии с Постановлением Правительства России от 16.03.2009 № 228

[1] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.

«О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»[1] (которым утверждено Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций) и Административным регламентом исполнения Роскомнадзором государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям федерального законодательства в области персональных данных (утв. Приказом Минкомсвязи России от 14.11.2011 № 312[2]).

Помимо вышеизложенного, в соответствии с ч. 8 ст.19 ФСТЭК и ФСБ в пределах своих полномочий (ФСБ – в части использования криптографических средств защиты информации, ФСТЭК – во всех остальных) вправе осуществлять контроль и надзор за выполнением организационных и технических мер при обработке персональных данных в государственных информационных системах персональных данных без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных. При этом ни ФСТЭК, ни ФСБ не наделены полномочиями по проведению контрольно-надзорных мероприятий в отношении операторов персональных данных, не являющихся государственными или муниципальными органами.

[1] Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Собрание законодательства РФ, 23.03.2009, № 12, ст. 1431.

[2] 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 14.11.2011 г. № 312 (ред. от 24.11.2014) // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2012. - № 9. – 27 февр.

6.2. Служебная тайна как вид защищаемой информации

Вопросы правового регулирования служебной информации ограниченного распространения на сегодняшний день являются объектом большого количества исследований и отличаются высокой полемичностью среди специалистов. Вызвано данное положение дел прежде всего отсутствием должного закрепления указанной категории информации в законодательстве Российской Федерации.

Правовую основу защиты служебной информации ограниченного распространения составляют следующие нормативные правовые документы:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ст. ст. 5, 9)

Указа Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

Постановления Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»;

ведомственных актов (в МВД РФ - Приказ МВД России от 09.11.2018 № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России»).

В соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» к *служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.* Руководители федеральных органов исполнительной власти в пределах своей компетенции определяют категорию должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения и обеспечивать ее защиту. Данное определение не раскрывает сущности рассматриваемой категории информации даже по той причине, что непонятно что такое служебная необходимость и кто ее определяет. Анализируя данное определение становится очевидным, что законодатель в служебной информации относит, во-первых ту информацию, которая образуется в деятельности государственного органа и связывает ее со служебной необходимость, и, во-вторых, ту информацию, которая поступает в официальном информационном обмене в орган государственной власти,

например, налоговую тайну, аудиторскую тайну, тайну следствия, тайну судопроизводства, тайну совещания судей и др.

Служебная тайна распространяется на информацию, которая находится в распоряжении органов власти (государственных и муниципальных), является охраноспособной и обладает свойством конфиденциальности.

Выделяют два *вида сведений, на которые распространяется служебная тайна органов власти:*

сведения, созданные непосредственно самим органом власти, в отношении которых действует требование конфиденциальности, обеспечивающее их сохранность от незаконного доступа;

сведения, касающиеся других лиц, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности (конфиденциальные сведения о гражданах и организациях).

Признаки информации, относящейся к служебной тайне:

получена представителем государственного органа (или органа местного самоуправления) в силу исполнения обязанностей по службе в случаях и порядке, установленных федеральным законом;

не относится к информации, составляющей государственную тайну;

не подпадает под перечень сведений, доступ к которым не может быть ограничен;

отнесена федеральным законом к служебной информации о деятельности государственных органов, доступ к которой ограничен по закону или в силу служебной необходимости (собственная служебная тайна);

является охраноспособной информацией, отвечающей требованию конфиденциальности другого лица (коммерческая тайна, банковская тайна, тайна частной жизни, профессиональная тайна).

В настоящее время в законодательстве имеется правовой пробел по ограничению доступа к информации, составляющей служебную тайну. Необходимо в срочном порядке принять Федеральный закон "О служебной тайне", в котором следует закрепить понятие служебной тайны, определить перечень сведений, составляющих служебную тайну, определить права и обязанности субъектов по предоставлению указанных сведений и охране их конфиденциальности, а также установить виды и случаи наступления юридической ответственности за нарушение соответствующего законодательства.

6.3. Коммерческая тайна как вид защищаемой информации

Законодательство о коммерческой тайне включает: Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»[1], а также главу 75 IV части Гражданского кодекса РФ[2] «Право на секрет производства (ноу-хау)».

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

Информация, составляющая коммерческую тайну, – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» в ст. 5 содержит *перечень сведений, которые не могут составлять коммерческую тайну*. Это сведения:

1) содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической 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, в том числе об охране труда, о показателях

[1] Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» // Собрание законодательства РФ. - 2004. - №32.

[2] Гражданский Кодекс Российской Федерации. Часть первая: Федеральный закон от 30.11.1994 № 51-ФЗ // Собр. законодательства РФ. 1994. № 32. Ст. 3301.

производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

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, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

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.

На практике к информации, составляющей коммерческую тайну (секрет производства), принято относить:

а) содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности организации, которое должно быть отнесено к коммерческой тайне в любом случае - в силу п. 4 статьи 10 Федерального закона от 21 ноября 1996 года № 129-ФЗ «О бухгалтерском учете»[1];

б) информацию о полезных моделях, промышленных образцах, изобретениях и иных объектах интеллектуальной собственности, находящихся на стадии разработки (регистрации);

в) информацию о партнерах и клиентах (покупателях, поставщиках, посредниках, контрагентах и др.), об условиях заключаемых сделок, ценообразовании, предлагаемых скидках, акциях, расчетах цен и формируемых на основе этих сведений клиентских базах;

г) информацию личного характера - все сведения об источниках доходов, личной жизни руководства и главного бухгалтера, членов их семей, адреса, расписание деловых встреч, данные об их контактных телефонах, пагубных привычках, маршрутах передвижений и т. д.;

д) информацию о технических средствах охраны имущества организации, системах охранной и иной сигнализации, методах и приемах обеспечения безопасности деятельности организации, местах хранения материальных ценностей.

[1] Федеральный закон от 21 ноября 1996 г. № 129 "О бухгалтерском учете" // // Собрание законодательства Российской Федерации. - 1996 г. - № 48. - Ст. 5369.

В соответствии с п.1 ст. 6. Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»[1] обладатель информации, составляющей коммерческую тайну обязан предоставить данные сведения органу государственной власти, иному государственному органу, органу местного самоуправления. Предоставление осуществляется на безвозмездной основе при наличии мотивированного требованию, которое подписано уполномоченным должностным лицом, содержит цель и правовое основание затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

На основании ст.6.1 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» обладатель информации, составляющей коммерческую тайну, имеет право:

1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;

2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;

3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;

4) требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;

5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;

6) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, *работодатель обязан*:

1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих

[1] Федеральный закон от 29 июля 2004 года №98-ФЗ «О коммерческой тайне» // Собрание законодательства РФ. - 2004. - №32.

трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, *работник обязан*:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их 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, составляющей коммерческую тайну и 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.

6.4. Правовое регулирование защиты сведений, связанных с профессиональной деятельностью

Информацию, защита которой является обязанностью субъекта в силу выполняемых им профессиональных полномочий, принято относить к категории *профессиональная тайна. Субъектом* профессиональной тайны может выступать и физическое, и юридическое лица.

К профессиональной тайне относятся следующие виды тайн:

- банковская тайна;
- нотариальная тайна;
- адвокатская тайна;
- врачебная тайна;
- тайна страхования;
- тайна исповеди;
- иные виды тайн.

Банковская тайна.

В ГК РФ[1], а именно в ст. 857 установлена обязанность банка гарантировать тайну следующих сведений:

банковского счета;

банковского вклада;

операций по счету;

о клиенте.

Указанные сведения предоставляются:

самим клиентам или их представителям;

в бюро кредитных историй;

государственным органам и их должностным лицам (в определенных случаях).

Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»[2] в ст. 26 устанавливает обязанность служащих кредитной организации хранить в тайне следующие сведения о клиентах и корреспондентах:

об операциях;

о счетах;

о вкладах;

об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

К банковской тайне относятся сведения, касающиеся:

клиентов банка – их паспортные данные, сведения о местонахождении (местожительстве), банковских реквизитах юридического лица, сведения о его руководстве;

банковского счета клиента – вид счета, дата его открытия, номер счета, данные о суммах на счете, количество счетов клиента, сведения о владельце счета;

банковского вклада – вид вклада, сумма вклада, порядок начисления и размер процентов, срок вклада;

операция по счетам и вкладам клиентов – валюта счета, суммы, зачисляемые и списываемые со счета, документы, на основании которых проводятся операции по счету, выписки со счетов;

корреспондентов банка – валюта и сумма операций, условия и даты сделок;

иной деятельности банка, связанной с управлением финансами, внутренними технологическими процессами, имеющие ценность для банка в силу неизвестности их третьим лицам.

---

[1] Гражданский Кодекс Российской Федерации. Часть первая: Федеральный закон от 30.11.1994 № 51-ФЗ // Собр. законодательства РФ. 1994. № 32. Ст. 3301.

[2] Федеральный закон от 2 декабря 1990 г. № 395-1 (в ред. от 08.04.2008 № 46-ФЗ, с изм. от 27.10.2008 № 175-ФЗ) "О банках и банковской деятельности" // СЗ РФ. 05.02.1996. № 6. Ст. 492; Российская газета. 1996. 10 февраля. № 27.

Банковская тайна должна строго соблюдаться банком и не подлежит разглашению, а также опубликованию в средствах массовой информации и передаче третьим лицам.

Рассматриваемые сведения могут быть предоставлены без нарушения законодательства следующим органам и организациям:

судам и арбитражным судам;

Счетной палате Российской Федерации;

налоговым органам;

таможенным органам;

федеральному органу исполнительной власти в области финансовых рынков;

Пенсионному фонду;

Фонду социального страхования;

органам принудительного исполнения судебных актов, актов других органов и должностных лиц;

органам предварительного следствия по делам, находящимся в их производстве;

органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений;

уполномоченному органу, осуществляющему меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, в случаях, порядке и объеме, которые предусмотрены Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем»[1];

органу валютного контроля.

С согласия юридического лица, индивидуального предпринимателя или физического лица информация по их операциям представляется банками в целях формирования кредитных историй в бюро кредитных историй в соответствии с Федеральным законом "О кредитных историях".

Банки и организации, в силу федеральных законов имеющие отношение к банковской тайне, а также их служащие, имеющие отношение к банковской тайне в силу исполнения своих должностных обязанностей, несут ответственность за разглашение банковской тайны.

Врачебная тайна.

В соответствии со ст. 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ[2] *врачебную тайну составляют следующие сведения*:

о факте обращения гражданина за оказанием медицинской помощи;

состоянии его здоровья и диагнозе;

---

[1] Федеральный закон от 7 августа 2001 г. № 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" // Собрание законодательства Российской Федерации. - 13 августа 2001 г. - №33 (Часть I). - Ст. 3418.

[2] Федеральный закон от 21.11.2011 г. № 323-ФЗ (ред. от 23.07.2013 г.) Об основах охраны здоровья граждан в Российской Федерации // Собрание законодательства РФ. - 2011. - № 48. - ст. 6724.

иные сведения, полученные при его медицинском обследовании и лечении.

По общему правилу *не допускается разглашение сведений, составляющих врачебную тайну,* в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей.

При этом *допускается разглашение* указанных сведений с письменного согласия гражданина или его законного представителя в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

Законодательством установлены случаи, когда *предоставление сведений, составляющих врачебную тайну, возможно без согласия гражданина* (п. 4 ст. 13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ[1]). Таковыми являются:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

3.1) в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача, либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

4) в случае оказания медицинской помощи несовершеннолетнему больного наркоманией при оказании ему наркологической помощи или при медицинском освидетельствовании несовершеннолетнего в целях установления состояния наркотического либо иного токсического

[1] Федеральный закон от 21.11.2011 г. № 323-ФЗ (ред. от 23.07.2013 г.) Об основах охраны здоровья граждан в Российской Федерации // Собрание законодательства РФ. - 2011. - № 48. - ст. 6724.

опьянения (за исключением установленных законодательством Российской Федерации случаев приобретения несовершеннолетними полной дееспособности до достижения ими восемнадцатилетнего возраста), а также несовершеннолетнему, не достигшему возраста пятнадцати лет (в соответствии с ч. 2 ст. 54 № 323-ФЗ[1]), для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти и федеральных государственных органов, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с ч. 6 ст. 34.1 Федерального закона от 4 декабря 2007 года № 329-ФЗ «О физической культуре и спорте в Российской Федерации»[2] несчастного случая с лицом, проходящим спортивную подготовку и не состоящим в трудовых отношениях с физкультурно-спортивной организацией, не осуществляющей спортивной подготовки и являющейся заказчиком услуг по спортивной подготовке, во время прохождения таким лицом спортивной подготовки в организации, осуществляющей спортивную подготовку, в том числе во время его участия в спортивных соревнованиях, предусмотренных реализуемыми программами спортивной подготовки;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности.

Нарушение врачебной тайны – это разглашение ее хотя бы одному лицу, умышленное или неосторожное (небрежное хранение документации

[1] Федеральный закон от 21.11.2011 г. № 323-ФЗ (ред. от 23.07.2013 г.) Об основах охраны здоровья граждан в Российской Федерации // Собрание законодательства РФ. - 2011. - № 48. - ст. 6724.

[2] Федеральный закон «О физической культуре и спорте в РФ» от 04 декабря 2007 № 329-ФЗ (ред. от 27 июля 2010) // Российская газета. - 2007. - 08 декабря. - № 276.

или беседа медиков в людном месте). Необходимый обмен информацией в ходе оказания специалистами медицинской помощи не рассматривается как нарушение врачебной тайны. Вся информация в медицинских документах гражданина также является врачебной тайной.

Адвокатская тайна.

Статья 8 Федерального закона от 31.05.2002 № 63-ФЗ (ред. от 11.07.2011) «Об адвокатской деятельности и адвокатуре в Российской Федерации» [1] определяет, что *адвокатской тайной* являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Режим адвокатской тайны распространяется на следующие сведения:

факт обращения к адвокату;

о доказательствах, подготовленных адвокатом по делу;

сведения, переданные доверителем адвокату;

сведения о самом доверителе, которые стали известны адвокату в ходе рассмотрения дела;

содержание юридических рекомендаций доверителю;

делопроизводство адвоката по делу;

условия соглашения об оказании юридической помощи;

иные сведения, связанные с оказанием юридических услуг.

Гарантии обеспечения адвокатской тайны реализуются в следующем:

адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах дела, имеющегося у него в производстве;

оперативно-розыскные мероприятия и следственные действия в отношении адвоката проводятся только на основании судебного решения, причем полученные сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей (за исключением орудия преступления, а также предметов, запрещенных к обращению или с ограниченным оборотом).

Федеральным законом «Об адвокатской деятельности и адвокатуре в Российской Федерации» установлено: «помощник адвоката и стажер адвоката обязаны хранить адвокатскую тайну».

Нотариальная тайна (тайна нотариальных действий).

Согласно ст. 5 Основ законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462-1) *нотариусу при исполнении служебных обязанностей, лицу, замещающему временно отсутствующего нотариуса, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и*

[1] Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» // Собрание законодательства Российской Федерации. - 2002г. - №23. - Ст.2102.

после сложения полномочий или увольнения, за исключением случаев, предусмотренных настоящими Основами. Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия.

Справки о совершенных нотариальных действиях выдаются по требованию суда, прокуратуры, органов следствия в связи с находящимися в их производстве уголовными, гражданскими или административными делами, а также по требованию судебных приставов-исполнителей в связи с находящимися в их производстве материалами по исполнению исполнительных документов.

Тайна страхования.

В соответствии со ст. 946 ГК Российской Федерации [1] *тайну страхования* составляют сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц, полученные страховщиком в результате своей профессиональной деятельности.

В соответствии с Законом РФ от 27.11.1992 № 4015-1 «Об организации страхового дела в Российской Федерации»[2] в качестве лица, обязанного сохранять тайну страхования, могут выступать как юридические, так и физические лица - *страховые агенты и страховые брокеры.*

Доступ к сведениям, составляющим тайну страхования, на законных основаниях *имеют*: 1) представитель страхователя (выгодоприобретателя) - на основании нотариально удостоверенной доверенности; 2) орган дознания и предварительного следствия - по находящимся в его производстве уголовным делам; 3) суд - на основании определения суда по находящимся в его производстве делам; 4) прокурор - на основании постановления о производстве проверки в пределах его компетенции по находящимся у него на рассмотрении материалам.

Тайна усыновления.

В соответствии со ст.139 Семейного кодекса РФ[3] *тайна усыновления ребенка охраняется законом*. Тайны усыновления распространяется на:
судей, вынесших решение об усыновлении, и всех работников суда, причастных к судебному делопроизводству, и всех участвующих в рассмотрении дела лицам;
должностные лица, осуществляющие государственную регистрацию усыновления (работники органов записи актов гражданского состояния, представители органов опеки и попечительства, медицинские работники).

---

[1] Гражданский Кодекс Российской Федерации. Часть первая: Федеральный закон от 30.11.1994 № 51-ФЗ // Собр. законодательства РФ. 1994. № 32. Ст. 3301.

[2] Закон РФ от 27 ноября 1992 г. № 4015-1 "Об организации страхового дела в Российской Федерации" Российская газета. - 12 января 1993 г.

[3] Семейный кодекс Российской Федерации от 29 декабря 1995 г. № 223-ФЗ // Собрание законодательства Российской Федерации от 1 января 1996 г. № 1 ст. 16.

Тайна исповеди.

Тайна исповеди – самостоятельный вид охраняемых законом тайн, одна из гарантий свободы вероисповедания.

Обеспечение тайны исповеди является внутренним делом священника, юридической ответственности за ее разглашение он не несет. Согласно ч. 2 ст. 51 Конституции РФ[1] и ч. 7 ст. 3 Федерального закона «О свободе совести и религиозных объединениях»[2] священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Согласно церковному каноническому праву, священник не может нарушить тайну исповеди ни при каких условиях. Это строго запрещено 120-м правилом Номоканона при Большом Требнике[3]: за открытие греха исповедовавшегося духовный отец отстраняется на три года от служения, и каждый день должен класть сто поклонов.

Контрольные вопросы:

1. Что понимается под термином «персональные данные»?
2. Какие сведения могут относиться к категории персональных данных?
3. Какими нормативными документами регулируются вопросы защиты персональных данных?
4. Раскройте содержание основных категорий персональных данных?
5. Что понимается под термином «информация, составляющая служебную тайну»?
6. Какими нормативными документами регулируются вопросы защиты служебной тайны?
7. Какая информация относится к служебной информации ограниченного распространения?
8. Что такое коммерческая тайна?
9. Что понимается под термином «информация, составляющая коммерческую тайну»?
10. Какими нормативными правовыми документами регулируются вопросы защиты коммерческой тайны?
11. Какие сведения не могут составлять коммерческую тайну?
12. Что относится к мерам по обеспечению конфиденциальности информации, составляющей коммерческую тайну?

---

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)// Собрание законодательства РФ, 04.08.2014, № 31, ст.

[2] Федеральный закон от 26.09.1997 № 125-ФЗ (ред. от 02.07.2013) «О свободе совести и о религиозных объединениях»// Собрание законодательства РФ. 1997. № 39. Ст. 4465; 2013. № 27. Ст. 3477.

[3] Номоканон при Большом Требнике: его история и тексты, греческий и славянский, с объяснительными и критическими примечаниями : монография / А.С. Павлов. – Репр. изд. 1897 г. – Москва ; Берлин : Директ-Медиа, 2016. – 540 с.

13. Какая информация относится к категории профессиональная тайна?

14. Приведите характеристику банковской тайны как вида защищаемой информации.

15. Приведите характеристику врачебной тайны как вида защищаемой информации.

16.Приведите характеристику адвокатской тайны как вида защищаемой информации.

17. Приведите характеристику нотариальной тайны как вида защищаемой информации.

18. Приведите характеристику тайны страхования как вида защищаемой информации.

19. Приведите характеристику тайны усыновления и тайны исповеди как видов защищаемой информации.

ГЛАВА 7. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

7.1. Защита интеллектуальной собственности в системе правового регулирования информационной безопасности

Впервые понятие интеллектуальной собственности используется с момента учреждения в 1967 году в Стокгольме Всемирной организации интеллектуальной собственности (ВОИС). В советском законодательстве термин «интеллектуальная собственность» появился впервые в Законе СССР «О собственности в СССР» (6 марта 1990 года). В российском законодательстве данный термин был утвержден Конституцией РФ [1], принятой в декабре 1993 года, и первой частью Гражданского кодекса РФ от 30.11.1994 № 51-ФЗ[2].

В настоящее время законодательство в области защиты прав на результаты интеллектуальной деятельности включает в себя положения части четвертой ГК (от 18 декабря 2006 г., вступившего в силу с 1 января 2008 г.), международные договоры РФ, другие нормативные правовые акты, регулирующие отношения в области интеллектуальной собственности.

Интеллектуальные права или право интеллектуальной собственности – юридический термин, обозначающий совокупность прав, которыми

[1] "Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)// Собрание законодательства РФ, 04.08.2014, № 31, ст.

[2] Гражданский кодекс Российской Федерации (часть первая) (статьи 1 - 453) (с изменениями на 18 июля 2019 года) (редакция, действующая с 1 октября 2019 года)

обладают лицо или лица (авторы или иные правообладатели) на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации.

Термин «интеллектуальная собственность» определён в ст. 1225 части четвертой Гражданского кодекса РФ как список результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, которым предоставляется правовая защита. Термин «интеллектуальные права» определён в ст. 1226 как права на «результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (результаты интеллектуальной деятельности и средства индивидуализации)».

Результатами интеллектуальной собственности, в соответствии с п.1 ст. 1225 ГК РФ[1], являются произведения науки, литературы и искусства, программы для электронных вычислительных машин (программы для ЭВМ), базы данных, исполнения, фонограммы, сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания), изобретения, полезные модели, промышленные образцы, селекционные достижения, топологии интегральных микросхем, секреты производства (ноу-хау), фирменные наименования, товарные знаки и знаки обслуживания, наименования мест происхождения товаров, коммерческие обозначения.

В настоящее время интеллектуальная собственность как подотрасль гражданского права состоит из следующих институтов:

авторское право;

охрана смежных прав;

патентное право;

законодательство о средствах индивидуализации участников гражданского оборота, товаров и услуг;

законодательство о нетрадиционных объектах ИС (научные открытия, ноу-хау);

законодательство о защите против недобросовестной конкуренции.

7.2. Основы авторского права

Авторское право (англ. copyright) – часть гражданского права, регулирующая отношения, возникающие в связи с использованием произведений науки, литературы, искусства.

Авторское право представляет собой совокупность правовых норм, регулирующих отношения, возникающие между объектами и субъектами права в отношении созданного произведения.

Авторское право распространяется на произведения:

[1] Гражданский кодекс Российской Федерации (часть первая) (статьи 1 - 453) (с изменениями на 18 июля 2019 года) (редакция, действующая с 1 октября 2019 года)

обнародованные на территории РФ или необнародованные, но находящиеся в какой-либо объективной форме на территории РФ, – признается за авторами (их правопреемниками) независимо от их гражданства;

обнародованные за пределами территории РФ или необнародованные, но находящиеся в какой-либо объективной форме за пределами территории РФ, — признается за авторами, являющимися гражданами РФ (их правопреемниками);

обнародованные за пределами территории РФ или необнародованные, но находящиеся в какой-либо объективной форме за пределами территории РФ, – признается на территории РФ за авторами (их правопреемниками) – гражданами других государств в соответствии с международными договорами РФ. Произведение также считается впервые опубликованным в РФ, если в течение 30 дней после даты первого опубликования за ее пределами оно было опубликовано на территории РФ.

Распространение авторского права возникает в силу факта создания произведения. Для возникновения и осуществления авторского права не требуется регистрации произведения, иного специального оформления или соблюдения каких-либо формальностей.

Объектами авторского права являются:

первичные произведения, в том числе литературные (включая программы для ЭВМ);

вторичные, то есть производные произведения (переводы, обработки, аннотации, рефераты т.п.), а также сборники и другие составные произведения, представляющие собой по подбору и расположению материала результаты творческого труда (энциклопедии, антологии, базы данных).

К числу произведений, не являющихся объектами авторского права, относятся:

официальные документы, их официальные переводы;

сообщения о событиях и фактах, имеющих информационный характер;

идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.

Субъектами авторского права являются правообладатели, среди которых выделяются:

автор;

наследник автора;

любое физическое или юридическое лицо, которое обладает исключительными имущественными правами, полученными в силу закона или договора.

Автором признается физическое лицо или группа физических лиц, в результате творческой деятельности которых создан результат интеллектуальной деятельности.

В случае, если база данных, состоит из материалов, не являющихся объектами авторского права, авторское право принадлежит лицам, ее создавшим. В противном случае необходимо согласие авторов на включение этих данных в общую базу.

Не признаются авторами физические лица:

не внесшие личного творческого вклада;

оказавшие только техническую, организационную или материальную помощь, в том числе в оформлении документов.

Знак охраны авторского права состоит из трех элементов:

латинской буквы (С) в окружности;

имени (наименования) обладателя исключительных авторских прав;

года первого опубликования произведения.

Автору принадлежат следующие права:

личные неимущественные права, а именно право авторства, право на имя, псевдоним или анонимность, право на неприкосновенность, целостность как самого объекта, так и их названий, право на обнародование произведения, право на защиту своей репутации;

имущественные права: исключительные права на использование произведения в любой форме и любым способом, в частности право на воспроизведение, распространение, публичный показ, передачу в эфир, перевод, переработку.

Личные неимущественные права принадлежат автору независимо от его имущественных прав и сохраняются за ним в случае уступки исключительных прав на использование произведения.

Имущественные права могут быть переданы полностью или частично любому лицу по договору, который заключается в письменной форме и должен устанавливать объемы и способы использования объекта, порядок и размеры выплаты вознаграждения, срок действия. Имущественные права переходят по наследству.

В случае, если результат интеллектуального творчества создан при выполнении служебных обязанностей, заданий работодателя или работ по договору с заказчиком, права принадлежат работодателю или заказчику, если договором не предусмотрено иное. Получение вознаграждения, порядок его выплаты и размер указываются в договоре между автором и работодателем.

Срок действия авторского права определяется в течение всей жизни автора и 70 лет после его смерти.

Для произведения, выпускаемого периодически анонимно или под псевдонимом, авторское право действует 70 лет с момента выпуска в свет.

За нарушение авторских и смежных прав предусмотрены следующие виды ответственности:
гражданско-правовая;
административная;
уголовная.

При нарушении требований закона, признаваемых как нарушение исключительных прав, их правообладатель имеет право:
требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации;
требовать возмещения морального вреда;
обратиться для защиты своих прав в суд, арбитражный суд, третейский суд, органы прокуратуры, органы дознания, органы предварительного следствия в соответствии с их компетенцией.

Нарушителем авторского права является лицо, не выполняющее требования законодательства в отношении исключительных прав правообладателей, в том числе ввозящее в Россию экземпляры программ или баз данных, изготовленных без разрешения их правообладателей.

Контрафактными являются экземпляры произведения, изготовление или использование которых влечет за собой нарушение авторского права, в том числе ввозимые в Россию из государства, в котором эти произведения никогда не охранялись или перестали охраняться.

Программы для ЭВМ и базы данных являются объектами авторского права. Программы для ЭВМ охраняются как произведения литературы, а базы данных – как сборники.

Не являются объектами авторского права:
идеи и принципы, лежащие в основе программы для ЭВМ;
базы данных или какой-либо их элемент, в том числе идеи и принципы организации интерфейса и алгоритма;
языки программирования.

Особенностью авторского права на программы для ЭВМ и базы данных является то, что право не связано с правом собственности на их материальный носитель и любая передача прав на материальный носитель не влечет за собой передачи каких-либо прав на программы для ЭВМ и базы данных. Автору программы для ЭВМ и базы данных принадлежат личные неимущественные и имущественные права.

Основными нарушениями авторских прав иных правообладателей в отношении программы для ЭВМ или базы данных, материалов и оборудования, используемых для их воспроизведения, являются:

изготовление;

воспроизведение;

распространение;

продажа, ввоз или иное использование;

выпуск под своим именем чужой программы или базы данных.

В отношении контрафактных экземпляров программ, базы данных, материалов и оборудования, используемых для их воспроизведения, суд или арбитражный суд может вынести решение:

о конфискации, их уничтожении;

о передаче в доход бюджета РФ, передаче истцу по его просьбе в счет возмещения убытков;

об аресте в порядке, установленном законом;

об уголовной ответственности.

7.3. Основы патентного права

Патентное право – подотрасль гражданского права, регулирующая правоотношения, связанные с созданием и использованием (изготовление, применение, продажа, иное введение в гражданский оборот) объектов интеллектуальной собственности, охраняемых патентом.

На основании ст. 1349 ГК РФ[1] *объектами патентных прав* являются:

изобретения;

полезные модели;

промышленные образцы.

Изобретение – новое, обладающее существенными отличиями техническое решение задачи в любой области экономики, социального развития, культуры, науки, техники, обороны, дающее положительный эффект и удовлетворяющее некоторым критериям патентоспособности.

К *объектам изобретения* относятся:

устройство;

способ;

вещество;

штамм микроорганизма;

культуры клеток растений и животных;

применение известного ранее устройства, способа, вещества, штамма по новому назначению.

Не признаются патентоспособными изобретениями:

научные теории и математические методы;

методы организации и управления хозяйством;

условные обозначения, расписания, правила;

методы выполнения умственных операций;

алгоритмы и программы для вычислительных машин;

проекты и схемы планировки сооружений, зданий, территорий;

решения, касающиеся только внешнего вида изделий, направленные на удовлетворение эстетических потребностей;

топологии интегральных микросхем;

[1] Гражданский кодекс Российской Федерации (часть первая) (статьи 1 - 453) (с изменениями на 18 июля 2019 года) (редакция, действующая с 1 октября 2019 года)

сорта растений и породы животных;

решения, противоречащие общественным интересам, принципам гуманности и морали.

Полезные модели – технические решения, представляющие собой конструктивное выполнение средств производства и предметов потребления, а также их составных частей и отвечающие требованиям патентоспособности.

Не подлежат правовой защите как полезные модели:

способы;

вещества;

штаммы микроорганизмов;

культуры клеток растений и животных, а также их применение по новому назначению.

Промышленные образцы – художественно-конструкторские решения, определяющие внешний вид изделия. Предоставление правовой защиты промышленному образцу осуществляется при соответствии его требованиям патентоспособности.

Не признаются патентоспособными промышленными образцами:

решения, обусловленные исключительно технической функцией изделия;

объекты архитектуры (кроме малых архитектурных форм), промышленных, гидротехнических и других стационарных сооружений;

печатная продукция как таковая;

объекты неустойчивой формы из жидких, газообразных, сыпучих или им подобных веществ;

изделия, противоречащие общественным интересам, принципам гуманности и морали.

Правовая охрана не предоставляется изобретениям, полезным моделям, промышленным образцам, признанным государством секретными, и обращение с ними регулируется специальным законодательством РФ.

Правовая защита рассмотренных объектов промышленной собственности предоставляется в случае их удовлетворения показателям патентоспособности. К таким показателям относится *новизна, наличие изобретательского уровня, промышленная применимость, оригинальность.*

Для *изобретения* установлены такие показатели, как *новизна, наличие изобретательского уровня, промышленная применимость.*

Новизна изобретения: в случае если существенные признаки формулы изобретения включают сведения, ставшие общедоступными в мире до даты приоритета. Изобретательский уровень означает, что изобретение должно быть результатом творческой, а не основанной на распространенных представлениях или общедоступных знаниях работы.

Показатель промышленной применимости предполагает установление того, что техническое решение может быть использовано в промышленности, сельском хозяйстве, здравоохранении и других областях деятельности.

Для полезной модели приняты показатели новизны и промышленной применимости.

Новая полезная модель – модель, в которой совокупность ее существенных признаков неизвестна из уровня техники. Промышленно применимая полезная модель – модель, которая может быть использована в промышленности, сельском хозяйстве, здравоохранении и других отраслях.

Для промышленного образца приняты показатели возможности многократного воспроизведения образца путем производства соответствующего изделия, новизны, оригинальности и промышленной применимости.

Новый промышленный образец – образец, у которого совокупность его существенных признаков, определяющих эстетические и (или) эргономические особенности изделия, неизвестна из сведений, ставших общедоступными в мире до даты приоритета промышленного образца. Оригинальный промышленный образец — образец, у которого его существенные признаки обусловливают творческий характер эстетических особенностей изделия. Промышленно применимый промышленный образец – образец, который может быть многократно воспроизведен путем изготовления соответствующего изделия.

Основными *субъектами* патентного права являются авторы (изобретения, полезной модели, промышленного образца), патентообладатели, их правопреемники.

Автор – любое физическое лицо, творческим трудом которого созданы изобретение, полезная модель, промышленный образец, селекционное достижение. При создании объекта промышленной собственности несколькими физическими лицами все они считаются его авторами. Порядок пользования правами, принадлежащими авторам, определяется соглашением между ними. При отсутствии такого соглашения каждый автор может использовать изобретение по своему усмотрению, но не вправе передать свои права третьему лицу без согласия остальных авторов.

Не признаются авторами физические лица, не внесшие личного творческого вклада в создание объекта промышленной собственности, оказавшие автору только техническую, организационную или материальную помощь, либо только способствовавшие оформлению прав на его использование.

Патентообладатель – лицо, владеющее патентом на изобретение, промышленный образец, свидетельством на полезную модель,

селекционное достижение и вытекающими из патента (свидетельства) исключительными правами на использование указанных объектов.

Патентообладателями могут быть:

авторы изобретения, полезной модели, промышленного образца селекционного достижения; их наследники или иные правопреемники;

физические и юридические лица (при условии их согласия), указанные автором или его правопреемником в заявлении, поданном в Патентное ведомство до момента регистрации изобретения, полезной модели, промышленного образца;

работодатели – в отношении объектов промышленной собственности, созданных работником в связи с выполнением служебного задания, с выплатой последнему вознаграждения в размере и на условиях специального соглашения между ними.

Право авторства является неотчуждаемым личным правом и охраняется бессрочно.

Правообладателем выступает лицо, которому выдан патент. Это может быть:

автор (авторы) изобретения, полезной модели, промышленного образца;

физические и юридические лица, которые указаны автором (авторами) или его (их) правопреемником в заявке на выдачу патента либо в заявлении, поданном в патентное ведомство до момента регистрации изобретения, полезной модели, промышленного образца

Патентные права подтверждаются особыми документами:

патентами на изобретение или промышленный образец;

свидетельством на полезную модель.

Начало срока действия патента (свидетельства) определяется с момента поступления авторской заявки на изобретение (полезную модель, промышленный образец) в патентное ведомство, где фиксируются год, месяц, день, час и минута.

Сроки действия документов:

патент на изобретение действует в течение 20 лет;

патент на промышленный образец — 10 лет;

свидетельство на полезную модель — 5 лет.

Сроки действия патента на промышленный образец и свидетельство на полезную модель могут быть продлены, но не более чем соответственно на 5 лет и 3 года.

На государственном уровне правом патентообладания пользуется Федеральный фонд изобретений РФ, который приобретает их на договорной основе и реализует в интересах государства.

Процесс патентования начинается с подачи заявки на изобретение. Заявка включает следующие документы:

заявление на бланке установленной формы, выдачу которого производит Федеральный институт промышленной собственности (ФИПС);

описание изобретения, раскрывающее его с полнотой, достаточной для промышленного применения;

формула изобретения;

чертежи и иные материалы;

реферат.

Заявка на выдачу патента подается автором, работодателем или их правопреемником в патентное ведомство. Затем проводится экспертиза (в течении 2-х месяцев). После принятия решения о выдаче патента патентное ведомство публикует в своем официальном бюллетене сведения о выдаче патента. Одновременно с публикацией оно вносит в Государственный реестр изобретений РФ, Государственный реестр полезных моделей РФ или Государственный реестр промышленных образцов РФ соответственно изобретение, полезную модель или промышленный образец и выдает патент лицу, на имя которого он направляется.

В течение 2 месяцев со дня поступления заявки в патентное ведомство заявитель имеет право вносить в ее материалы исправления и уточнения без изменения сущности изобретения.

При положительном результате экспертизы принимается решение о выдаче патента. В случае отказа решение может быть обжаловано в апелляционной палате в течение 3 месяцев со дня его получения или копий материалов, на которые приводятся ссылки в решении. Возражение должно быть рассмотрено в 4-месячный срок. Решение апелляционной палаты может быть обжаловано в Высшей патентной палате в течение 6 месяцев с момента ею получения. Решение последней является окончательным.

При положительном решении о выдаче патента сведения о нем публикуются в официальном издании патентного ведомства, а само изобретение вносится в Государственный реестр изобретений РФ.

Нарушением исключительного права патентообладателя считается:

любое хозяйственное использование охраняемых сведений, вплоть до хранения продукта, содержащего объект промышленной собственности;

несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью продукта, содержащего запатентованное изобретение, полезную модель, промышленный образец;

применение способа, охраняемого патентом на изобретение, или введение в хозяйственный оборот либо хранение с этой целью продукта, изготовленного непосредственно способом, охраняемым патентом на изобретение. При этом новый продукт считается полученным запатентованным способом при отсутствии доказательств противного.

Контрольные вопросы:

1. Что понимается под термином «интеллектуальная собственность»?
2. Что понимается под термином «интеллектуальные права»?
3. Какими нормативными документами регулируются вопросы интеллектуальной собственности?
4. Что относится к результатам интеллектуальной собственности?
5. Что такое авторское право?
6. Перечислите объекты авторского права?
7. Перечислите субъекты авторского права.
8. Кто признается автором и соавтором?
9. Какие права принадлежат автору произведения?
10. Что такое исключительное право?
11. Каков срок действия исключительного права?
12. Каковы особенности защиты программ для ЭВМ и баз данных институтом авторского права?
13. Что такое патентное право?
14. Перечислите объекты патентного права.
15. Перечислите субъекты патентного права.
16. Кто признается автором объектов патентного права?
17. Кто может являться патентообладателем?
18. Какими документами подтверждаются патентные права, каков срок их действия?
19. Что является нарушением исключительного права патентообладателя?

ГЛАВА 8. ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВОВЫХ НОРМ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Понятие юридической ответственности

Вопросы определения юридической ответственности в сфере информационной безопасности является одной из важнейших задач деятельности государства и его компетентных органов.

Юридическая ответственность является разновидностью социальной ответственности лица. Наступление юридической ответственности связано с нарушением юридических норм.

Юридическая ответственность выражается в необходимости виновному лицу подвергнуться мерам государственного воздействия, претерпеть определенные отрицательные последствия. Другими словами,

юридическая ответственность – это способ реагирования государства на правонарушение.

Применительно к лицу юридическая ответственность выражается в виде наступления отрицательных последствий материального, морального, личного, организационного, физического характера (лишение или ограничение свободы, исправительные работы, конфискация имущества, штраф, арест, лишение права занимать определенные должности, смертная казнь).

Признаки юридической ответственности:

предусмотрена действующим законодательством (уголовным, гражданским, административным и др.);

наступает в случае наличия полного состава правонарушения;

опирается на государственное принуждение;

выражается в определенных отрицательных последствиях;

возлагается и реализуется в установленной законом процессуальной форме, осуществляется уполномоченными на то компетентными органами и должностными лицами.

Основаниями юридической ответственности являются необходимые условия привлечения к юридической ответственности:

нормативное основание – это наличие действующей нормы права, устанавливающей определенное деяние как правонарушение.

фактическое основание – это фактически совершенное правонарушение;

процессуальное основание – это вступивший в силу акт уполномоченного государственного органа или должностного лица о привлечении нарушителя к ответственности.

Функциями юридической ответственности являются: 1) карательная; 2) штрафная; 3) предупредительная, или превентивная; 4) воспитательная; 5) компенсационная, или правовосстановительная.

Принципами юридической ответственности являются:

принцип законности;

принцип обоснованности;

принцип неотвратимости;

принцип справедливости;

принцип гуманизма;

презумпция невиновности.

8.2. Виды юридической ответственности

Отдельные исследователи отмечают, что виды юридической ответственности соответствуют видам правонарушений. Рассмотрим более подробно понятие правонарушения, его состав и виды.

Правонарушение – это общественно вредное, противоправное, виновное деяние, за которое законом предусмотрена юридическая ответственность.

Признаки правонарушения:

вред для общества;

противоправность;

виновность;

реальность правонарушения;

наказуемость.

Состав правонарушения – это совокупность установленных законом элементов, наличие которых позволяет квалифицировать деяние как определенное правонарушение.

Состав правонарушения включает четыре взаимосвязанных компонента, при отсутствии хотя бы одного из которых отсутствует состав правонарушения.

Объект правонарушения – это общественные отношения, которым правонарушением причинен вред. Это различного рода публичные и частные ценности: правопорядок, окружающая природная среда, собственность, права и свободы человека и т.п.

Субъект правонарушения – это деликтоспособный индивид или организация, совершившие правонарушение. Для физического лица деликтоспособность включает достижение определенного возраста и вменяемость, для организации – наличие статуса юридического лица.

Объективная сторона правонарушения – это характеристика противоправного деяния: время, место, орудие, способ, обстановка совершения правонарушения, размер и характер вредных последствий, причинная связь между деянием и вредными последствиями. Таким образом, объективная сторона представляет собой единство трех элементов – противоправного деяния, вреда и причинной связи между ними.

Субъективная сторона правонарушения – это сознательно – волевые признаки правонарушения, основным из которых является вина (умысел или неосторожность), а факультативными – мотивы и цели правонарушителя. Мотивы представляют собой побудительные причины, которыми руководствовался нарушитель, цели – конечный результат, к которому стремился правонарушитель.

Все правонарушения принято делить на две группы — преступления и проступки. Главными критериями их деления являются:

значимость регулируемого правом общественного отношения, ставшего объектом противоправного посягательства (жизнь человека, материальные ценности и т.д.);

размер причиненного ущерба;

способ, время и место совершения противоправного деяния;

личность правонарушителя.

По Уголовному кодексу *преступлением* признается виновное, общественно опасное деяние (действие или бездействие), запрещенное уголовным законом под угрозой наказания (ст.14 УК РФ). За совершение уголовных преступлений предусмотрены следующие виды наказаний: штраф; лишение права занимать определенные должности или заниматься определенной деятельностью; лишение специального, воинского или почетного звания, классного чина и государственных наград; обязательные работы; исправительные работы; ограничение по военной службе; ограничение свободы; принудительные работы; арест; содержание в дисциплинарной воинской части; лишение свободы на определенный срок; пожизненное лишение свободы; смертная казнь. (ст.44 УК РФ).

Все проступки классифицируются применительно к отраслям права:

административное — таковым признается посягающее на государственный или общественный порядок, собственность, права и свободы граждан, на установленный порядок управления противоправное виновное действие или бездействие, за которое законодательством предусмотрена административная ответственность.

За совершения административных правонарушений предусмотрены административные взыскания: предупреждение; административный штраф; конфискация орудия совершения или предмета административного правонарушения; лишение специального права, предоставленного физическому лицу; административный арест; административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства; дисквалификация; административное приостановление деятельности; обязательные работы; административный запрет на посещение мест проведения официальных спортивных соревнований в дни их проведения.

Гражданские проступки – это нарушение гражданами или организациями имущественных или неимущественных прав, принадлежащих субъектам права. Различают договорные и внедоговорные правонарушения. Первые связаны с нарушением обязательств стороной гражданско-правового договора (взыскание: возмещение убытка), вторые — с несоблюдением или неисполнением требований гражданско-правовых норм (взыскание: опровержение).

Дисциплинарные проступки представляют собой противоправные деяния субъекта трудового права, состоящие в неисполнении, нарушении трудовых обязанностей и запрещенные санкциями, содержащимися в нормах законодательства о труде. Совершая дисциплинарный проступок, правонарушитель нарушает трудовую, учебную, служебную, производственную, воинскую дисциплину (прогулы, опоздания на работу, пропуски учебных занятий, невыполнение распоряжений администрации). Санкции норм права выражаются в следующих взысканиях: замечание, выговор, строгий выговор, перевод на низшую должность, увольнение и пр.

На основании рассмотренных видов правонарушений выделим следующие *виды юридической ответственности*:

гражданско-правовая ответственность (гражданское правонарушение);

дисциплинарная ответственность (дисциплинарный, служебный проступок);

административная ответственность (административный проступок);

уголовная ответственность (преступление)[1].

На практике большое значение приобретает правильная классификация ответственности, так как для гражданской ответственности характерна презумпция ответственности, а для уголовной и административной – презумпция невиновности.

Уголовная ответственность применяется за совершение преступлений как наиболее общественно опасных деяний. В Российской Федерации их исчерпывающий перечень определен Уголовным кодексом. Наказания назначаются только по приговору суда. К уголовной ответственности в России привлекаются лишь физические лица.

Административная ответственность – применяется за совершение административных проступков. К административной ответственности привлекаются как физические лица, так и организации за нарушения норм отраслей публичного права. Субъектами, имеющими полномочия на привлечение к административной ответственности, являются многочисленные государственные органы исполнительной власти и их должностные лица. Административная ответственность применяется не в порядке подчиненности, не влечет судимости и увольнения с работы.

Дисциплинарная ответственность применяется за нарушения трудовой, служебной, учебной, воинской дисциплины в рамках линейных отношений «работник – работодатель» или «начальник – подчиненный». В Российской Федерации нормативную базу дисциплинарной ответственности составляет Трудовой кодекс РФ, Федеральный закон «О полиции» и другие нормативные акты. Таким образом, привлечение к дисциплинарной ответственности осуществляется в порядке служебной подчиненности. Дисциплинарные взыскания могут дополняться восстановительными мерами материального (имущественного) характера.

Гражданско-правовая ответственность применяется за нарушения гражданско-правовых обязательств. Данный вид ответственности в Российской Федерации регламентируется Гражданским кодексом РФ[2]. Сфера применения гражданско – правовой ответственности находится в отраслях частного права. Она всегда носит имущественный характер.

---

[1] Черданцев А.Ф., Кожевников С. Н. О понятии и содержании юридической ответственности // Правоведение. - 2001. - №5. - С. 29.

[2] Гражданский Кодекс Российской Федерации. Часть первая: Федеральный закон от 30.11.1994 № 51-ФЗ // Собр. законодательства РФ. 1994. № 32. Ст. 3301.

Главной целью здесь является полное возмещение вреда, причиненного правонарушением. Субъекты, привлекающие к гражданско-правовой ответственности, – это суды РФ и третейские суды.

8.3. Содержание УК РФ[1] и КоАП РФ[2] по вопросам ответственности в сфере информационной безопасности

8.3. Содержание УК РФ и КоАП РФ по вопросам ответственности в сфере информационной безопасности

№ п/п	№ и название статьи	Комментарий
Уголовный кодекс РФ		
1.	Статья 272. Неправомерный доступ к компьютерной информации	**объект:** общественные отношения, обеспечивающие сохранность и конфиденциальность компьютерной информации; **предмет:** охраняемая законом компьютерная информация (примечание 1 к статье) **объективная сторона:** неправомерный доступ к охраняемой законом компьютерной информации, которого является уничтожение, блокирование, модификация или копирование информации; **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **субъективная сторона:** виной в форме умысла. **квалифицирующие признаки:** а) причинение крупного ущерба (ущерб, сумма которого превышает один миллион рублей); б) совершение из корыстной заинтересованности; в) совершение группой лиц по предварительному сговору; г) совершение организованной группой; д) совершение с использованием своего служебного положения;

[1] Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации - 17 июня 1996 г. - № 25 - Ст. 2954.

[2] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. - 7 января 2002 г. - №1. - Ст. 1.

		е) наступление тяжких последствий или создание угрозы их наступления.
2.	Статья 273. Создание, использование и распространение вредоносных компьютерных программ	**объект:** общественная безопасность и общественный порядок, а также совокупность общественных отношений по правомерному и безопасному использованию информации; **предмет:** вредоносные программы для ЭВМ или машинные носители, содержащие такие программы. **объективная сторона:** факт создания компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **субъективная сторона:** виной в форме прямого умысла. **квалифицирующие признаки:** а) причинение крупного ущерба (ущерб, сумма которого превышает один миллион рублей); б) совершение из корыстной заинтересованности; в) совершение группой лиц по предварительному сговору; г) совершение организованной группой; д) совершение с использованием своего служебного положения; е) наступление тяжких последствий или создание угрозы их наступления.
3.	Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-	**объект:** общественная безопасность и общественный порядок, а также совокупность общественных отношений по правомерному и безопасному использованию информации; **объективная сторона:** действия или бездействия, заключающиеся в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо

	телекоммуникационных сетей	информационно-телекоммуникационных сетей и оконечного оборудования либо правил доступа к информационно-телекоммуникационным сетям, предполагается два последствия, наступающих друг за другом и причинно связанных, а именно уничтожение, блокирование, модификация или копирование компьютерной информации, что, в свою очередь, вызывает причинение крупного ущерба. **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **субъективная сторона:** вина и в форме умысла, и в форме неосторожности. **квалифицирующие признаки:** а) наступление тяжких последствий или создание угрозы их наступления.
4.	Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации	**объект:** безопасность критической информационной инфраструктуры Российской Федерации, т.е. состояние ее защищенности от любого воздействия программными или программно-техническими средствами, которое способно привести к нарушению ее функционирования и (или) нарушению безопасности обрабатываемой ею информации. **предмет:** компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. Специфический предмет: объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-

		космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности. **объективная сторона:** ч. 1 ст. 274.1 УК РФ – действия: создание, использование или распространение компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры; ч.2. ст. 274.1 УК РФ – неправомерный доступ, повлекший уничтожение, блокирование, модификация, копирование информации, содержащейся в критической информационной инфраструктуре, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры ч.3. ст.274.1 УК РФ – нарушение: 1) правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации; информационных систем; информационно-телекоммуникационных сетей; автоматизированных систем управления; сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации; 2) правил доступа к указанным средствам, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи. Перечисленные действия /бездействия должны повлечь причинение вреда критической информационной инфраструктуре Российской Федерации. **субъект:** ч. ч. 1 и 2 ст. 274.1 УК РФ – физическое вменяемое лицо, достигшее возраста 16 лет; ч. 3 ст. 274.1 УК РФ – может быть как общий, в части правил доступа к ресурсам, так и специальный -

		в части соблюдения правил эксплуатации соответствующих средств, систем и сетей. **субъективная сторона:** вина и в форме умысла, и в форме неосторожности. **квалифицирующие признаки:** 1) совершение группой лиц по предварительному сговору; 2) совершение организованной группой; 3) совершение с использованием своего служебного положения; 4) наступление тяжких последствий или создание угрозы их наступления.
5.	Статья 137. Нарушение неприкосновенности частной жизни	**объект:** основной - общественные отношения, складывающиеся по поводу реализации конституционного принципа неприкосновенности частной жизни, личной и семейной тайны (см. ч. 1 ст. 23, ч. 1 ст. 24 Конституции); факультативный - честь, достоинство и доброе имя человека. **предмет:** сведения о частной жизни лица, составляющие его личную или семейную тайну. **объективная сторона:** 1) незаконного собирания сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия; 2) незаконного распространения таких сведений без согласия лица; 3) распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, что характеризует не только само деяние, но и способ его совершения. **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, человек, которому ранее потерпевшим была доверена личная или семейная тайна и который впоследствии разгласил ее без согласия последнего **субъективная сторона**: вина в форме умысла. **квалифицирующие признаки:** 1) совершенные лицом с использованием своего служебного положения.

		Частью 3 ст. 137 УК РФ установлена повышенная уголовная ответственность за незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия.
6.	Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений	**объект:** общественные отношения, возникающие в связи с реализацией гражданами права на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ч. 2 ст. 23 КРФ). **предмет:** сведения, содержащиеся в переписке, телефонных переговорах, почтовых, телеграфных и иных (к примеру, факсовых) сообщениях; общие сведения о совершавшихся лицом телефонных переговорах, сделанных почтовых, телеграфных и иных сообщениях. **объективная сторона:** выполнение любых незаконных действий, нарушающих тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан Преступление окончено с момента совершения деяния, нарушающего указанную тайну. **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **субъективная сторона:** вина в виде прямого умысла. **квалифицирующие признаки:** - совершенное лицом с использованием своего служебного положения.

7.	Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации	**объект:** общественные отношения, возникающие в связи с реализацией права на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. **предмет:** специальные технические средства, предназначенные для негласного получения информации. **объективная сторона:** альтернативные действия: а) производство специальных технических средств, предназначенных для негласного получения информации; б) их приобретение; в) их сбыт. **субъект: прямой умысел.** **субъективная сторона:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **Примечание к ст.138.1:** 1. Под специальными техническими средствами, предназначенными для негласного получения информации, в настоящем Кодексе понимаются приборы, системы, комплексы, устройства, специальные инструменты для проникновения в помещения и (или) на другие объекты и программное обеспечение для электронных вычислительных машин и других электронных устройств для доступа к информации и (или) получения информации с технических средств ее хранения, обработки и (или) передачи, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя. 2. К специальным техническим средствам, предназначенным для негласного получения информации, не относятся находящиеся в свободном обороте приборы, системы, комплексы, устройства, инструменты бытового назначения, обладающие функциями аудиозаписи, видеозаписи, фотофиксации и (или) геолокации, с открыто расположенными на них органами управления таким функционалом или элементами индикации, отображающими режимы их использования, или наличием на них маркировочных обозначений, указывающих на

		их функциональное назначение, и программное обеспечение с элементами индикации, отображающими режимы его использования и указывающими на его функциональное назначение, если им преднамеренно путем специальной технической доработки, программирования или иным способом не приданы новые свойства, позволяющие с их помощью получать и (или) накапливать информацию, составляющую личную, семейную, коммерческую или иную охраняемую законом тайну, без ведома ее обладателя.
8.	Статья 140. Отказ в предоставлении гражданину информации	**объект:** основной объект - общественные отношения, возникающие в связи с обязанностью органов государственной власти и органов местного самоуправления, а также их должностных лиц обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы (часть 2 статьи 24 Конституции РФ); факультативный объект - честь, достоинство и деловая репутация граждан. **объективная сторона:** альтернативные деяния: а) отказ в предоставлении гражданину информации; б) уклонение должностного лица от предоставления информации; в) предоставление заведомо неполной информации; г) предоставление заведомо ложной информации, которые должны причинить вред правам и законным интересам гражданина. Последствия в виде вреда правам и законным интересам граждан. **субъект:** специальный - должностные лица органов государственной власти РФ, органов местного самоуправления, предприятий, учреждений, организаций независимо от форм собственности, в компетенцию которых входит предоставление соответствующей информации. **субъективная сторона:** умышленная форма вины.
9.	Статья 146. Нарушение	**объект:** основной - общественные отношения, возникающие в связи с реализацией гражданами конституционного права на свободу научного,

	авторских и смежных прав	литературного и художественного творчества; факультативный - честь, достоинство и деловая репутация автора и иного правообладателя. **предмет:** объекты авторского права и объекты смежных прав. **объективная сторона:** характеризуется: а) действием в виде присвоения авторства (ч. 1), повлекшим крупный ущерб (если стоимость экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав превышают сто тысяч рублей, а в особо крупном размере - один миллион рублей.); б) незаконным использованием объектов авторского права или смежных прав либо приобретением, хранением, перевозкой контрафактных экземпляров произведений или фонограмм (ч. 2), совершенными в крупном размере. **субъект:** вменяемое физическое лицо, достигшее 16-летнего возраста. **субъективная сторона:** вина в форме прямого умысла. **квалифицирующие признаки:** деяние, совершенное: 1) группой лиц по предварительному сговору или организованной группой; 2) в особо крупном размере; 3) лицом с использованием своего служебного положения, -
10.	Статья 147. Нарушение изобретательских и патентных прав	**объект:** общественные отношения, возникающие по поводу создания и использования изобретений, полезных моделей и промышленных образцов. **объективная сторона:** альтернативные действия: а) незаконным использованием изобретения, полезной модели или промышленного образца; б) разглашением без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них; в) присвоением авторства; г) принуждением к соавторству, причинившие автору или заявителю сущности

		изобретения, полезной модели, промышленного образца крупного ущерба (имущественный (материальный) ущерб). **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **субъективная сторона:** вина в форме прямого или косвенного умысла.
11.	Статья 155. Разглашение тайны усыновления (удочерения)	**объект:** интересы семьи, родителей и детей, право на неприкосновенность частной жизни, личной и семейной тайны. **объективная сторона:** разглашение тайны усыновления (удочерения) вопреки воле усыновителя. Под разглашением понимается раскрытие кому-либо конфиденциальной информации об усыновлении (удочерении) независимо от формы сообщения (устно, письменно). **субъект:** а) специальный субъект - лицо, обязанное хранить факт усыновления (удочерения) как служебную или профессиональную тайну; б) общий субъект - лицо, достигшее возраста 16 лет, разгласившее тайну усыновления (удочерения) из корыстных или иных низменных побуждений. **субъективная сторона:** *вина* в форме прямого умысла: *мотив* - корыстные или иные низменные побуждения, но при условии, что деяние совершено лицом, не обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну. В случае наличия такой обязанности лицо привлекается к уголовной ответственности независимо от мотивации поведения.
12.	Статья 159.3. Мошенничество с использованием платежных карт	**объект:** общественные отношения, сложившиеся в сфере социального обеспечения населения. **объективная сторона:** хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты, путем обмана уполномоченного

		работника кредитной, торговой или иной организации. Преступное деяние считается законченным с момента получения лицом товаров или суммы денег, а равно приобретения им юридического права на распоряжение данными товарами или деньгами. **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **субъективная сторона:** вина в форме прямого умысла. **квалифицирующие признаки:** деяние: 1) совершенное группой лиц по предварительному сговору; 2) с причинением значительного ущерба гражданину; 3) лицом с использованием своего служебного положения; 4) совершенные организованной группой; 5) в особо крупном размере. *значительный ущерб* определяется с учетом его имущественного положения, но не может составлять менее пяти тысяч рублей; *крупный размер* - стоимость имущества, превышающая двести пятьдесят тысяч рублей; *особо крупный размер* - стоимость имущества, превышающая один миллион рублей.
13.	Статья 159.6. Мошенничество в сфере компьютерной информации	**объект:** общественные отношения, сложившиеся в сфере электронного документооборота. **объективная сторона:** хищение чужого имущества, равно приобретения права на него путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Преступное деяние считается законченным с момента получения виновным суммы денег (чужого имущества), а равно приобретения им юридического права на распоряжение такими деньгами (имуществом).

		субъект: физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. **субъективная сторона:** вина в форме прямого умысла. **квалифицирующие признаки:** деяние: 1) совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину; 2) лицом с использованием своего служебного положения; 3) в крупном размере; 4) с банковского счета, а равно в отношении электронных денежных средств; 5) совершенные организованной группой; 6) в особо крупном размере.
14.	Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	**объект:** общественные отношения, возникающие в сфере обращения информации, составляющей коммерческую, налоговую или банковскую тайну. **предмет:** информация, составляющая коммерческую, налоговую или банковскую тайну **объективная сторона:** - собирание путем похищения документов, подкупа или угроз, а равно иным незаконным способом (ч.1); - незаконные разглашение или использование без согласия их владельца (ч.2) **субъект:** любое лицо, вменяемое, достигшее 16-летнего возраста (ч.1); специальный - лицо, которому тайна сведений была доверена или стала известна по службе или работе (ч. 2 - 4). **субъективная сторона:** вина в форме умысла. **квалифицирующие признаки:** деяние: 1) причинившее крупный ущерб; 2) совершенные из корыстной заинтересованности; 3) повлекшие тяжкие последствия.
15.	Статья 185.1. Злостное уклонение	**объект:** основной объект -экономическая деятельность, установленная

	от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах	законодательством; факультативный объект - материальные интересы гражданина, организации или государства. **предмет:** находящаяся на соответствующем материальном носителе информация, содержащая данные об эмитенте, о его финансово-хозяйственной деятельности, о ценных бумагах, сделках и иных операциях с ценными бумагами. объективная сторона: 1) предоставлении инвестору или контролирующему органу неполной или ложной информации; 2) лицо, обязанное обеспечить информацией об эмитенте, его финансово-хозяйственной деятельности и ценных бумагах, сделках и иных операциях с ценными бумагами инвестора или контролирующий орган, злостно уклоняется от предоставления данной информации. Действие/бездействие должно причинить гражданам (гражданину), организациям (организации) или государству крупный ущерб (сумма, превышающую 1 млн. руб.). **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста и наделенное дополнительным (специальным) признаком - правом предоставления информации об эмитенте инвестору или контролирующему органу либо обязанностью обеспечить указанной информацией инвестора или контролирующий орган. **субъективная сторона:** вина в форме умысла.
16.	Статья 185.6. Неправомерное использование инсайдерской информации	**объект:** основной - установленный законом порядок использования инсайдерской информации, дополнительный - имущественные интересы граждан, организаций, государства; **объективная сторона:** признаком объективной стороны использование инсайдерской информации становится в двух случаях: - при совершении сделок за счет принадлежащего виновному либо иному лицу имущества; - при рекомендации третьим лицам, обязывании или

		побуждении их иным образом к приобретению или продаже финансовых инструментов, иностранной валюты и (или) товаров. Использование инсайдерской информации является наказуемым, если оно причинило крупный ущерб гражданам, организациям или государству либо повлекло извлечение дохода (избежание убытков) в крупном размере (в сумме, превышающей три миллиона семьсот пятьдесят тысяч рублей). Преступление является оконченным с момента наступления указанных имущественных последствий. **субъект:** общий, им может быть не только лицо либо работник юридического лица, названные в ст. 4 Федерального закона от 27.07.2010 № 224-ФЗ, но и всякое иное вменяемое физическое лицо, достигшее 16 лет. **субъективная сторона:** вина в форме умысла.
17.	Статья 187. Неправомерный оборот средств платежей	**объект:** установленный порядок выпуска и обращения кредитных или расчетных карт, иных платежных документов, не являющихся ценными бумагами. **предмет:** кредитные карты, расчетные карты и иные платежные документы, не являющиеся ценными бумагами (платежные поручения, аккредитивы, платежные требования, инкассовые поручения). **объективная сторона:** изготовление, приобретение, хранение, транспортировка в целях использования или сбыта, а равно сбыт **субъект:** физическое вменяемое лицо, достигшее на момент совершения преступления 16-летнего возраста. **субъективная сторона:** вина в форме прямого умысла. **квалифицирующие признаки:** деяния, совершенные организованной группой
18.	Статья 205.2. Публичные призывы к осуществлению террористической деятельности,	**объект:** отношения по поддержанию мер общественной безопасности. **объективная сторона:** публичные призывы к осуществлению террористической деятельности или публичном оправдании терроризма.

	публичное оправдание терроризма или пропаганда терроризма	**субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16 лет. **субъективная сторона:** вина в форме прямого умысла. **квалифицирующие признаки:** деяния, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет». **Примечания. 1.** В настоящей статье под публичным оправданием терроризма понимается публичное заявление о признании идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании. 1.1. В настоящей статье под пропагандой терроризма понимается деятельность по распространению материалов и (или) информации, направленных на формирование у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности. 2. В настоящей статье под террористической деятельностью понимается совершение хотя бы одного из преступлений, предусмотренных статьями 205 - 206, 208, 211, 220, 221, 277, 278, 279, 360, 361 настоящего Кодекса.
19.	Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов	**объект:** психическое здоровье населения, общественная нравственность. **предмет:** порнографические материалы и предметы, за исключением материалов или предметов с порнографическими изображениями несовершеннолетних, которые являются предметом преступления, предусмотренного ст. 242.1 УК. **объективная сторона:** ч. 1: а) незаконное изготовление в целях распространения, публичной демонстрации или рекламирования; б) незаконное перемещение в целях распространения, публичной демонстрации или рекламирования; в) незаконное распространение; г) незаконная

		публичная демонстрация; д) незаконное рекламирование; ч. 2: а) распространение, публичная демонстрация или рекламирование порнографических материалов или предметов среди несовершеннолетних; б) вовлечение несовершеннолетнего в оборот порнографической продукции. **субъект:** физическое вменяемое лицо, достигшее к моменту совершения преступления 16 лет. **субъективная сторона:** вина в форме прямого умысла.
20.	Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних	**объект:** психическое здоровье населения, общественная нравственность. **предмет:** материалы либо предметы с порнографическим изображением несовершеннолетних девочек и (или) мальчиков, т.е. они содержат непристойное, циничное изображение половой жизни несовершеннолетних, с акцентированием контакта половых органов. Элементами порнографии являются сексуальные извращения, сексуальные контакты, сексуальные манипуляции, извращенное стимулирование непристойного содержания. **объективная сторона:** 1) изготовление; 2) приобретение; 3) хранение; 4) перемещение через Государственную границу РФ; 5) распространение; 6) публичная демонстрация; 7) рекламирование материалов или предметов. **субъект:** ч. 1, — вменяемое физическое лицо, достигшее 16-летнего возраста. В случае совершения указанных действий специальным субъектом — родителем несовершеннолетнего, изображенного в материалах порнографического характера, либо иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетних (усыновитель, опекун, попечитель, член приемной семьи), педагогом или другим работником образовательного, воспитательного, лечебного либо иного учреждения, обязанным осуществлять надзор за

		несовершеннолетним, действия такого лица подлежат квалификации по п. «а» ч. 2 комментируемой статьи. **субъективная сторона:** вина в форме прямого умысла. **квалифицирующие признаки:** деяния, совершенные: а) в отношении лица, не достигшего четырнадцатилетнего возраста; б) группой лиц по предварительному сговору или организованной группой; в) с извлечением дохода в крупном размере; г) с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет»), **Примечания. 1.** Под *материалами и предметами с порнографическими изображениями несовершеннолетних* в настоящей статье и статье 242.2 УК РФ понимаются материалы и предметы, содержащие любое изображение или описание в сексуальных целях: полностью или частично обнаженных половых органов несовершеннолетнего; несовершеннолетнего, совершающего либо имитирующего половое сношение или иные действия сексуального характера; полового сношения или иных действий сексуального характера, совершаемых в отношении несовершеннолетнего или с его участием; совершеннолетнего лица, изображающего несовершеннолетнего, совершающего либо имитирующего половое сношение или иные действия сексуального характера. 2. *Не являются* материалами и предметами с порнографическими изображениями несовершеннолетних материалы и предметы, содержащие изображение или описание половых органов несовершеннолетнего, если такие материалы и предметы имеют историческую, художественную или культурную ценность либо

		предназначены для использования в научных или медицинских целях, либо в образовательной деятельности в установленном федеральным законом порядке.
21.	Статья 242.2. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов	**Объект и предмет** см. ст. 242.1 УК РФ **объективная сторона:** 1) фотосъемка несовершеннолетнего; 2) киносъемка несовершеннолетнего; 3) видеосъемка несовершеннолетнего; 4) привлечение несовершеннолетнего в качестве исполнителя для участия в зрелищном мероприятии порнографического характера. **субъект:** физическое вменяемое лицо, достигшее 18-летнего возраста. **субъективная сторона:** вина в форме прямого умысла. **квалифицирующие признаки:** деяние, совершенное: а) в отношении двух или более лиц; б) группой лиц по предварительному сговору или организованной группой; в) в отношении лица, не достигшего четырнадцатилетнего возраста; г) с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)
22.	Статья 275. Государственная измена	**объект:** внешняя безопасность РФ. **объективная сторона:** а) шпионаж; б) выдача государственной тайны; в) оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности РФ. **субъект:** гражданин Российской Федерации, вменяемый и достигший 16 лет. **субъективная сторона:** вина в форме прямого умысла. **Примечание.** Лицо, совершившее преступления, предусмотренные статьей 275, а также статьями 276 и 278 УК РФ, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным образом

		способствовало предотвращению дальнейшего ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления.
23.	Статья 276. Шпионаж	**объект:** внешняя безопасность РФ. **предмет:** сведения, составляющие государственную тайну, и иные сведения **объективная сторона:** - действия, выражающиеся в передаче, собирании, похищении или хранении в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну; - действия, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования против безопасности Российской Федерации; **субъект:** физическое вменяемое лицо, достигшее 16-летнего возраста, имеющее подданство другой страны, или лицо без гражданства (апатрид). **субъективная сторона:** вина в форме прямого умысла.
24.	Статья 283. Разглашение государственной тайны	**объект:** отношения по надлежащей сохранности государственной тайны в целях обеспечения безопасности суверенного государства. **предмет:** сведения, составляющие государственную тайну. **объективная сторона:** разглашение сведений, составляющих государственную тайну. **субъект:** специальный - любое лицо, которому государственная тайна была доверена в силу должностных обязанностей либо стала известна по службе или работе. **субъективная сторона:** ч. 1 совершается с любой формой вины. ч. 2 – неосторожная форма вины. **квалифицирующие признаки:** деяния, повлекшие тяжкие последствия.
25.	Статья 283.1. Незаконное	**объект:** безопасность государства.

	получение сведений, составляющих государственную тайну	**предмет:** сведения, составляющие государственную тайну. **объективная сторона:** получение сведений, составляющих государственную тайну следующими способами: похищение, обман, шантаж, принуждение, угрозы, а также другие способы (например, подкуп, отдача приказа или распоряжения, обязательных к исполнению). Перечень способов, указанных в статье, не является исчерпывающим. **субъект:** физическое, вменяемое лицо, достигшее 16-летнего возраста. **субъективная сторона:** вина в форме прямого умысла **квалифицирующие признаки:** деяние, а) совершено группой лиц; б) совершено с применением насилия; в) повлекло наступление тяжких последствий; г) совершено с использованием специальных и иных технических средств, предназначенных для негласного получения информации; д) сопряжено с распространением сведений, составляющих государственную тайну, либо с перемещением носителей таких сведений за пределы Российской Федерации
26.	Статья 284. Утрата документов, содержащих государственную тайну	**объект:** общественные отношения в сфере сохранения и защиты государственной тайны. **объективная сторона:** а) *деянием* (действием или бездействием), связанным с нарушением конкретных правил обращения с предметами и документами, составляющими государственную тайну; б) *последствием* (утратой указанных предметов и документов и наступлением тяжких последствий); в) *наличием причинной связи* между указанным деянием и последствиями. **субъект:** лицо, имеющее допуск к государственной тайне, т.е. ответственное за сохранность предмета (документа), либо допущенное к государственной тайне лицо,

		которому данный предмет или документ был передан по службе или работе. **субъективная сторона:** неосторожная форма вины.
27.	Статья 287. Отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации	**объект:** общественные отношения, обеспечивающие нормальное, в соответствии с задачами их деятельности, функционирование Федерального Собрания РФ и Счетной палаты РФ. **предмет:** официальные документы (справки, отчеты, аналитические обзоры, письменные ответы на запросы депутатов парламента и т.п.), содержащие заведомо неполную или ложную информацию по тем или иным вопросам, интересующим Федеральное Собрание или Счетную палату РФ. **объективная сторона:** а) неправомерный отказ предоставить информацию Федеральному Собранию или Счетной палате РФ (отказ представляет собой открытое проявление нежелания предоставить требуемую информацию без законных на то оснований); б) уклонение от предоставления запрашиваемой информации, что означает завуалированный отказ от предоставления необходимых сведений под различными надуманными предлогами (болезнь, отсутствие необходимых подписей, непоступление данных с мест, трудности обработки материала и т.д.); в) предоставление заведомо неполной информации, когда в предоставленных материалах или документах отсутствует существенная часть сведений, что искажает содержание информации; г) предоставлении заведомо ложной информации, т.е. сведений, не соответствующих действительности (неверные цифровые данные, искаженные факты и т.д.). **субъект:** должностное лицо, в чьи служебные обязанности входит предоставление информации перечисленным в законе органам. **субъективная сторона:** вина в форме прямого умысла **квалифицирующие признаки:**

		деяние, 1) совершенные лицом, занимающим государственную должность Российской Федерации или государственную должность субъекта Российской Федерации; 2) сопряжены с сокрытием правонарушений, совершенных должностными лицами органов государственной власти; 3) совершены группой лиц по предварительному сговору или организованной группой; 4) повлекли тяжкие последствия.
28.	Статья 310. Разглашение данных предварительного расследования	**объект:** общественные отношения, обеспечивающие тайну предварительного следствия и дознания как необходимое условие успешного осуществления расследования. **предмет** - данные предварительного расследования. **объективная сторона:** разглашении данных без согласия прокурора, следователя или лица, производящего дознание. **субъект:** лицо, которое в установленном законом порядке предупреждено о недопустимости разглашения данных предварительного расследования. **субъективная сторона:** вина в форме прямого умысла
29.	Статья 311. Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса	**объект:** основной - общественные отношения, обеспечивающие безопасность участия личности в производстве по уголовным делам как важное условие достижения цели (назначения) уголовного судопроизводства (ст. 6 УПК); факультативный - интересы личности, вовлеченной в производство по уголовным делам. **предмет:** сведения о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса (лица, производящего дознание, следователя, прокурора, эксперта, специалиста, понятого и т.д.) или в отношении их близких (см.

		Федеральные законы от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и др.). **объективная сторона:** действия по разглашению указанных сведений. **субъект:** лицо, которому сведения о мерах безопасности были известны или доверены в связи с его служебной деятельностью. **субъективная сторона:** как умышленная, так и неосторожная форма вины. **квалифицирующие признаки:** деяние, повлекшее тяжкие последствия.
30.	Статья 320. Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа	**объект:** управленческая деятельность, обеспечивающая безопасность жизни, здоровья, сохранность имущества лиц, взятых под защиту, а также лиц, осуществляющих ее. **предмет:** сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа либо его близких. **объективная сторона:** разглашение сведений о мерах безопасности. **субъект:** любое вменяемое физическое лицо 16-летнего возраста **субъективная сторона:** вина в форме прямого умысла **квалифицирующие признаки:** деяние, повлекшее тяжкие последствия.
Кодекс об административных правонарушениях РФ		
1.	Статья 5.39. Отказ в предоставлении информации	**объект:** общественные отношения, складывающиеся по поводу предоставления гражданам и организациям необходимой информации. Непосредственный объект - права граждан и организаций на получение информации. **предмет:** информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

		объективная сторона: а) в неправомерном отказе в предоставлении гражданину и (или) организации информации, предоставление которой предусмотрено федеральными законами; б) в несвоевременном ее предоставлении; в) в предоставлении заведомо недостоверной информации. **субъект:** специальный: должностное лицо, которое в силу занимаемого им положения располагает или может располагать информацией, затрагивающей права и свободы конкретного гражданина, права и обязанности организации **субъективная сторона:** умышленная форма вины
2.	Статья 5.53. Незаконные действия по получению и (или) распространению информации, составляющей кредитную историю	**Объект:** установленный законом порядок формирования, хранения и использования кредитных историй. **Предмет:** информация, составляющая кредитную историю. **Объективная сторона**: нарушение установленного порядка получения и (или) распространения информации, составляющей кредитную историю. **Субъект:** граждане, незаконно получившие или распространившие указанную информацию (например, рядовые сотрудники банка), так и должностные лица (например, руководители бюро кредитных историй). **Субъективная сторона:** характеризуется как умыслом, так и неосторожностью Примечание: одно из условий привлечения виновного лица к административной ответственности является отсутствие в противоправном деянии признаков состава уголовного преступления.
3.	Статья 5.59. Нарушение порядка рассмотрения обращений граждан	**Объект**: Общий - общественные отношения, связанные с рассмотрение обращений и заявлений граждан; Непосредственный объект - установленный законом порядок рассмотрения обращений и заявлений граждан, гарантируемый Конституцией РФ.

		Объективная сторона: противоправное действие или бездействие субъектов, уполномоченных рассматривать обращения. **Субъект**: специальный - руководители органов государственной власти, органов местного самоуправления, в которые адресуются обращения граждан, а также указаны должностные лица, которые постоянно, временно или по специальному полномочию осуществляют функции представителя власти либо выполняют организационно-распорядительные, административно-хозяйственные функции в этих органах и на которых возложены обязанности по рассмотрению обращений граждан **Субъективная сторона:** характеризуется умышленной либо неосторожной формой вины
4.	Статья 6.17. Нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию	**Объект:** здоровье населения. **Объективная сторона:** а) по ч. 1 выражается в совершении действий Нарушающих установленные требования распространения среди детей информации за исключением изготовления юридическим лицом материалов или предметов с порнографическими изображениями несовершеннолетних и оборота таких материалов или предметов; пропаганды нетрадиционных сексуальных отношений среди несовершеннолетних; незаконного распространения информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), или нарушения предусмотренных федеральными законами требований к распространению такой информации; нарушения установленного порядка распространения среди детей продукции СМИ, содержащей информацию, причиняющую вред их здоровью и (или) развитию. б) по ч. 2 выражается в форме бездействия - неприменения лицом, организующим доступ к распространяемой посредством информационно-телекоммуникационных сетей

		(в том числе сети Интернет) информации в местах, доступных для детей, административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию. в) по ч. 3 выражается в форме действия - размещения в информационной продукции для детей объявления о привлечении их к участию в создании информационной продукции, причиняющей вред их здоровью и (или) развитию. **Субъект**: вменяемое физическое лицо, достигшее 16 лет, должностное лицо, лицо, осуществляющее деятельность без образования юридического лица, юридическое лицо (ч. 1 статьи), лицо, осуществляющее деятельность без образования юридического лица, юридическое лицо (ч. 2 статьи), вменяемое физическое лицо, достигшее 16 лет, должностное лицо, юридическое лицо (ч. 3 статьи). **Субъективная сторона:** выражается в форме умысла и неосторожности.
5.	Статья 7.12. Нарушение авторских и смежных прав, изобретательских и патентных прав	**Объект:** а) отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права). б) отношения, возникающие в связи с наличием у лица изобретательских и патентных прав. **Предмет: объекты** авторских и смежных прав, изобретательских и патентных прав **Объективная сторона:** совершении субъектами правонарушения действий, направленных на незаконное использование произведения или фонограммы с нарушением авторских и смежных прав в целях извлечения доходов, а также незаконное использование изобретения, полезных моделей либо промышленных образцов до официального опубликования

		сведений о них, либо с присваиванием авторства или принуждением к соавторству. **Субъект:** физические лица (граждане, должностные лица) и юридические лица, нарушившие авторские и смежные права, изобретательские и патентные права. **Субъективная сторона:** прямой умысел и обязательное наличием цели - извлечение дохода.
6.	Статья 8.5. Сокрытие или искажение экологической информации	**Объект:** общественные отношения в сфере обеспечения населения экологической информацией, экологической безопасности, соблюдения конституционного права граждан на доступ к экологической информации и других связанных с ним прав. **Предмет:** экологическая информация о состоянии воды, воздуха, почвы, фауны, флоры, земли и отдельных природных объектов, вредных воздействиях или мерах, вредно влияющих или могущих влиять на эти объекты, видах деятельности или мерах, направленных на их охрану, включая административные меры и программы управления охраной окружающей среды. **Объективная сторона:** действия или бездействие, направленные на сокрытие или искажение имеющейся информации в сфере экологии. **Субъект:** должностные лица, юридические лица, обязанные в силу осуществляемой ими деятельности или возложенных полномочий предоставлять экологическую информацию. **Субъективная сторона:** умышленная или неосторожная форма вины, при этом искажение экологической информации возможно только с умышленной формой вины.
7.	Статья 13.3. Изготовление или установка радиоэлектронных средств и (или) высокочастотных устройств без специального	**Объект:** общее право на прием, обработку и передачу сообщений электросвязи. **Непосредственный объект:** конкретные отраслевые нормы в сфере связи, закрепленные соответствующими постановлениями Правительства РФ и приказами ведомственных органов исполнительной власти.

	разрешения (лицензии)	**Объективная сторона:** совершение запрещенных действий (самовольные проектирование, строительство, изготовление, приобретение, установка или эксплуатация указанных в статье средств и (или) устройств). **Субъект:** а) гражданин в возрасте от 16 лет; б) должностное лицо, назначенное приказом (либо решением собственника, учредителями); в) юридическое лицо, которое самостоятельно либо через филиалы, представительства осуществляет деятельность с нарушением, предусмотренным комментируемой статьей. **Субъективная сторона:** характеризуется прямым либо косвенным умыслом для должностных лиц. **Примечание.** 1. Под радиоэлектронными средствами в настоящей статье понимаются технические средства, состоящие из одного или нескольких радиопередающих, или радиоприемных устройств либо из их комбинации и вспомогательного оборудования и предназначенные для передачи или приема радиоволн. 2. Под высокочастотными устройствами понимаются оборудование или приборы, предназначенные для генерирования и местного использования радиочастотной энергии для промышленных, научных, медицинских, бытовых и других целей, за исключением применения в области электрической связи.
8.	Статья 13.6. Использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям	**Объект:** общественные отношения по использованию несертифицированных средств связи и предоставлению несертифицированных услуг. **Объективная сторона:** использование на сетях связи несертифицированных средств связи либо предоставлении несертифицированных услуг связи, если законом предусмотрена их обязательная сертификация. **Субъект**: граждане в возрасте от 16 лет, должностные лица, круг должностных

		обязанностей которых входит решение вопросов о применения средств связи либо оказание услуг связи; юридические лица, которые самостоятельно либо через филиалы, представительства осуществляют деятельность с нарушением, предусмотренным настоящей статьей **Субъективная сторона:** прямой умысел.
9.	Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных	**Объект:** общественные отношения, связанные с интересами персоны (личности) в информационной сфере. Непосредственный объект — право на персональные данные, имеет комплексную природу и формируется на основе множества международных, федеральных и локальных нормативных актов. **Объективная сторона:** нарушение порядка включает в себя все деяния (действия и бездействие), установленные федеральным законодательством, ведомственными и локальными нормами, которые не соответствуют правилам (регламенту) обращения с персональными данными. **Субъект:** а) гражданин в возрасте от 16 лет; б) должностное лицо, назначенное приказом (либо решением собственника, учредителями), в круг должностных обязанностей которого входит решение вопросов по осуществлению деятельности по защите информации о гражданах (персональных данных); в) юридическое лицо, которое самостоятельно либо через филиалы, представительства осуществляет деятельность с нарушением, предусмотренным настоящей статьей. **Субъективная сторона:** прямой умысел **Примечание**. За административные правонарушения, предусмотренные частями 8 и 9 настоящей статьи, статьями 13.31, 13.35 - 13.37, 13.39и 13.40 настоящего Кодекса, лица, осуществляющие предпринимательскую деятельность без образования юридического лица, несут

		административную ответственность как юридические лица.
10.	Статья 13.11.1. Распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера	**Объект:** общественные отношения, складывающиеся в области защиты информации содержащей ограничения дискриминационного характера **Объективная сторона:** все формы распространения информации. **Субъект**: а) гражданин в возрасте от 16 лет; б) должностное лицо, назначенное приказом (либо решением собственника, учредителями), в круг должностных обязанностей которого входит решение вопросов по осуществлению деятельности по защите информации о гражданах (персональных данных); в) юридическое лицо, которое самостоятельно либо через филиалы, представительства осуществляет деятельность с нарушением, предусмотренным настоящей статьей. **Субъективная сторона:** прямой умысел или неосторожность.
11.	Статья 13.12. Нарушение правил защиты информации	**Объект:** общественные отношения в области защиты информации. **Объективная сторона:** - в нарушении условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) (ч. 1); - в использовании несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну) (ч. 2); - в нарушении условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей

		государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну (ч. 3); - в использовании несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну (ч. 4); - в грубом нарушении условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) (ч. 5); - в нарушении требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, за исключением случаев, предусмотренных ч. ч. 1, 2 и 5 ст. 13.12 КоАП РФ (ч. 6); - в нарушении требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, за исключением случаев, предусмотренных ч. ч. 3 и 4 комментируемой статьи, если такие действия (бездействие) не содержат уголовно наказуемого деяния (ч. 7). **Субъект:** а) гражданин в возрасте от 16 лет; б) должностное лицо, назначенное приказом (либо решением собственника, учредителями), в круг должностных обязанностей которого входит решение вопросов по осуществлению деятельности по защите информации о гражданах (персональных данных); в) юридическое лицо, которое самостоятельно либо через филиалы, представительства осуществляет деятельность с нарушением, предусмотренным настоящей статьей.

		Субъективная сторона: прямой умысел или неосторожность. **Примечание.** Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.
12.	Статья 13.13. Незаконная деятельность в области защиты информации	**Объект:** отношения в сфере лицензирования деятельности по защите информации. **Объективная сторона:** а) занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна). б) более широкий круг противоправных деяний, осуществляемых без лицензии: занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии. **Субъект:** а) граждане, должностные и юридические лица. б) должностные, а также юридические лица, в отношении которых наряду со штрафом предусмотрена конфискация созданных без лицензии средств защиты информации, составляющей государственную тайну. **Субъективная сторона:** предполагает нарушение установленных правил лицензирования соответствующей деятельности как умышленное, так и по неосторожности.
13.	Статья 13.14. Разглашение информации с ограниченным доступом	**Объект:** отношения по поводу обеспечения порядка использования информации с ограниченным доступом при исполнении служебных или профессиональных обязанностей**.**

		Предмет: сведения, документы, файлы, базы данных и т.д., сведения, которые недоступны всем, доступны только тому лицу, которое ими владеет (доверитель), и лицу, которому их выдали для выполнения трудовых, служебных функций (конфидент). **Объективная сторона:** совершение нарушающих установленный правовой режим различных действий. (например: распространение, разглашение, передача информации за пределы ограниченного круга лиц, имеющих право законного доступа.) **Субъект:** а) гражданин в возрасте от 16 лет; б) должностное лицо, назначенное приказом (либо решением собственника, учредителями), в круг должностных обязанностей которого входит работа с информацией ограниченного доступа. **Субъективная сторона:** прямой умысел. **Примечание.** Адвокаты, совершившие административное правонарушение, предусмотренное настоящей статьей, несут административную ответственность как должностные лица.
14.	Статья 20.23. Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации	**Объект:** отношения в сфере обеспечения общественной безопасности, а также право граждан на неприкосновенность частной жизни, личную и семейную тайну, закрепленное в ст. 23 Конституции РФ. **Объективная сторона:** действия, выражающиеся в нарушении условий, предусмотренных лицензией, а также правил производства, хранения, продажи и приобретения специальных технических средств для негласного получения информации, в нарушении порядка разработки, ввоза в Российскую Федерацию и вывоза за ее пределы, а также порядка сертификации, регистрации и учета вышеуказанных специальных технических средств. **Субъект:** по ч. 1 данной статьи могут быть должностные и приравненные к ним по

		ответственности лица (руководители, другие работники, осуществляющие управленческие функции, индивидуальные предприниматели), а по ч. 2 - кроме перечисленных лиц и граждане. **Субъективная сторона:** прямой умысел.
15.	Статья 20.24. Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности	**Объект:** отношения в области обеспечения общественной безопасности. **Предмет:** специальные технические средства, предназначенные для негласного получения информации, в частной детективной или охранной деятельности **Объективная сторона:** действия, связанные с использованием в частной детективной или охранной деятельности специальных технических средств, предназначенных для негласного получения информации и не предусмотренных установленными законодательно перечнями. **Субъект:** физическое лицо, имеющее право осуществлять частную детективную либо охранную деятельность, а также руководитель частной охранной организации (должностное лицо). **Субъективная сторона:** прямой умысел.

Контрольные вопросы:

1. Что понимается под термином «юридическая ответственность»?
2. Перечислите признаки юридической ответственности.
3. Перечислите основания юридической ответственности.
4. Перечислите принципы юридической ответственности?
5. Что такое правонарушение и каковы его признаки?
6. Что такое состав правонарушения?
7. Перечислите виды правонарушений.
8. Перечислите и раскройте сущность видов юридической ответственности?
9. Приведите составы преступлений в области информационной безопасности, предусмотренные УК РФ.
10. Приведите составы правонарушений, предусмотренные КоАП РФ.

ТЕСТОВЫЕ ЗАДАНИЯ

1. Что такое защита информации?

а) Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

б) Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность.

в) Деятельность, направленная на предотвращение НСД к информации.

г) Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию.

2. Безопасность информации – это:

а) состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;

б) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;

в) реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность;

г) деятельность, направленная на предотвращение НСД к информации.

3. Система защиты информации – это:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) заранее намеченный результат защиты информации;

в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

г) порядок и правила применения определенных принципов и средств защиты информации.

4. Что такое «национальная безопасность»?

а) совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер;

б) система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу;

в) состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

г) состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

5. Информационная безопасность Российской Федерации – это:

а) состояние защищенности информации, циркулирующей в обществе;

б) состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;

в) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;

г) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

6. Что такое угроза безопасности информации в соответствии с Национальным стандартом РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006)?

а) потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам;

б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

в) состояние, в котором находится объект безопасности вследствие возникновения неблагоприятных факторов;

г) возможность реализации воздействия на информацию, обрабатываемую АС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты АС, приводящего к утрате, уничтожению или сбою функционирования носителя

информации, средства взаимодействия с носителем или средства его управления.

7. Техническая защита информации – это:
а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;
б) защита информации с помощью ее криптографического преобразования;
в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;
г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

8. Физическая защита информации – это:
а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;
б) защита информации с помощью ее криптографического преобразования;
в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;
г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

9. Правовая защита информации – это:
а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;
б) защита информации с помощью ее криптографического преобразования;
в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

10. Криптографическая защита информации – это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) защита информации с помощью ее криптографического преобразования;

в) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты;

г) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

11. Защита информации от утечки – это:

а) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

б) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации;

в) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами;

г) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению,

искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

12. Способ защиты информации – это:
а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;
б) заранее намеченный результат защиты информации;
в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;
г) порядок и правила применения определенных принципов и средств защиты информации.

13. Цель защиты информации – это:
а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;
б) заранее намеченный результат защиты информации;
в) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;
г) порядок и правила применения определенных принципов и средств защиты информации.

14. Замысел защиты информации – это:
а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;
б) деятельность по обеспечению защиты некриптографическими методами информации от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию;
в) совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация;
г) реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и

интеллектуального развития, а также защита информации, обеспечивающая личную безопасность.

15. Лицензирование в области защиты информации – это:
а) 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;
б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;
в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;
г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

16. Сертификация на соответствие требованиям по безопасности информации – это:
а) 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;
б) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации;
в) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации;
г) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

17. Аттестация объектов информатизации по требованиям безопасности информации – это:
а) комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата

соответствия» – подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации;
б) комплекс организационно-технических мероприятий, направленных на определение степени защищенности объекта информатизации от утечки по техническим каналам;
в) процедура анализа хранимой и обрабатываемой на объекте информатизации информации в интересах отнесения ее к защищаемой;
г) разделение защищаемой информации на именованные блоки с обеспечением возможности нахождения любого блока по его имени при решении задач защиты.

18. Защищаемая информация – это:
а) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;
б) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
в) информация, основанная на документах, фактах;
г) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

19. В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» под угрозой безопасности ПДн понимается:
а) совокупность условий факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн;
б) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности персональных данных;
в) стихийное бедствие или бедствие техногенного характера;
г) только стихийное бедствие.

20. Состояние информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на него право – это:
а) конфиденциальность;
б) целостность;
в) доступность;
г) помехоустойчивость.

21. Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право – это:
а) конфиденциальность;
б) целостность*;*
в) доступность;
г) безопасность.

22. Состояние информации, при котором субъекты, имеющие право доступа, могут реализовать его беспрепятственно – это:
а) конфиденциальность;
б) целостность*;*
в) доступность;
г) безопасность.

23. Объект защиты информации – это:
а) информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации;
б) совокупность объекта разведки, средства разведки, среды распространения сигнала.
в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
г) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

24. Носитель защищаемой информации – это:
а) свойство материальных объектов и явлений порождать многообразие состояний, которые посредством взаимодействий передаются другим объектам и запечатлеваются в их структуре;
б) смысловое содержание объективной информации об объектах и процессах материального мира, сформированное сознанием человека с помощью смысловых образов;

в) физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;
г) документ, содержащий достигнутые результаты или свидетельства осуществленной деятельности.

25. В соответствии с Федеральным законом от 28.12.2010 г. № 390-ФЗ «О безопасности» основными принципами обеспечения безопасности не являются:
а) соблюдение и защита прав и свобод человека и гражданина;
б) своевременность;
в) законность;
г) системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности.

26. Каким нормативным правовым документом утверждена Доктрина информационной безопасности?
а) Указ Президента РФ №136 от 16.03.2015 г.
б) ФЗ от 27.07.2006 г. №152
в) Постановление Правительства РФ №1233 от 3.11.1993 г.
г) Указ Президента РФ №646 от 6.12.2016 г.

27. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в:
а) Конституции РФ;
б) Гражданском кодексе РФ;
в) Доктрине информационной безопасности РФ;
г) Федеральном законе «Об информации, информационных технологиях и о защите информации».

28. В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные системы не включают в себя:
а) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов

субъектов Российской Федерации, на основании правовых актов государственных органов;
б) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;
в) иные информационные системы;
г) частные информационные системы.

29. Базовым законом, регулирующим информационные отношения, является:
а) ФЗ «О коммерческой тайне»;
б) Закон РФ «Об авторском праве и смежных правах»;
в) ФЗ «Об информации, информационных технологиях и защите информации»;
г) ФЗ «Об архивном деле».

30. Понятие информационной инфраструктуры Российской Федерации закреплено в:
а) Конституции РФ;
б) Федеральном законе от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
в) Доктрине информационной безопасности РФ;
г) не закреплено в нормативных правовых документах.

31. В соответствии с частью 3 статьи 29 Конституции Российской Федерации каждый имеет право свободно:
а) искать и распространять информацию любым способом;
б) искать, получать, передавать, производить и распространять информацию любым законным способом;
в) искать, получать, передавать, производить и распространять информацию любым способом;
г) получать и распространять информацию любым способом.

32. Федеральный закон от 27 июля 2006 г. «О персональных данных» не регулирует отношения, возникающие при:
а) обработке персональных данных, отнесенных к государственной тайне;
б) хранении, комплектовании, учете и использовании архивных документов;
в) обработке персональных данных, отнесенных к служебной тайне;
г) включении в Единый государственный реестр индивидуальных предпринимателей.

33. Каким нормативным правовым документом утвержден перечень сведений конфиденциального характера?

а) Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203;
б) Указом Президента Российской Федерации от 6 марта 1997 г. № 188;
в) Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870;
г) Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

34. Служебная информация ограниченного распространения – это:
а) акт законодательства, устанавливающий правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
б) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;
в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
г) информация, основанная на документах, фактах.

35. Допуск гражданина к сведениям, составляющим государственную тайну, может быть прекращен в случае:
а) перевода и приема гражданина на работу в подразделение по защите государственной тайны, шифровальные или мобилизационные органы;
б) возвращения из длительных (свыше 6 месяцев) заграничных командировок;
в) однократного нарушения им предусмотренных трудовым договором (контрактом) обязательств, связанных с сохранением государственной тайны;
г) вступления гражданина в брак, за исключением случаев, когда оба супруга работают в одной организации и имеют допуск по второй или третьей форме.

36. В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация – это:
а) сведения (сообщения, данные) независимо от формы их представления;
б) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
в) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
г) сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе

коммуникации.

37. Каким нормативным правовым документом утверждены правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?
а) Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203;
б) Указ Президента Российской Федерации от 6 марта 1997 г. № 188;
в) Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870;
г) Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

38. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под персональными данными понимается:
а) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
б) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
в) зафиксированная на материальном носителе информация о личности с реквизитами, позволяющими ее идентифицировать;
г) сведения, касающиеся личности, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности.

39. Какие категории персональных данных выделяет Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?
а) общедоступные персональные данные, специальные категории персональных данных, категории персональных данных, обрабатываемые в информационных системах персональных данных, биометрические персональные данные;
б) общедоступные персональные данные, специальные категории персональных данных, биометрические персональные данные и иные;
в) общедоступные персональные данные, категории персональных данных, обрабатываемые в информационных системах персональных данных;
г) данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

40. В соответствии с п. 3 ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите

информации» по категории доступа информация делится на:
а) общедоступную информацию и информацию с ограниченным доступом (информация ограниченного доступа);
б) открытую и конфиденциальную;
в) конфиденциальную и секретную;
г) служебную информацию ограниченного доступа и общедоступную.

41. Соблюдение каких правил входит в защиту правомочий обладателя информации?
а) соблюдение конфиденциальности информации – свойство информационной технологии (ИТ) обеспечивать раскрытие информации только в соответствии с правилами разграничения доступа (право распоряжения);
б) соблюдение целостности информации – свойство ИТ обеспечивать предоставление права модификации (уничтожения) информации только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность информации в условиях случайных ошибок или стихийных бедствий (право владения);
в) соблюдение доступности информации – свойство ИТ обеспечивать свободный доступ к информации по мере возникновения необходимости (право пользования);
г) соблюдение всех перечисленных правил.

42. Какая из перечисленных видов тайн относится к категории конфиденциальной информации?
а) государственная тайна, персональные данные, коммерческая тайна, служебная тайна;
б) персональные данные, коммерческая тайна, служебная тайна;
в) государственная тайна, коммерческая тайна, служебная тайна;
г) секретные сведения, совершенно секретные сведения, сведения особой важности.

43. Каков срок засекречивания сведений, составляющих государственную тайну?
а) 10 лет;
б) 20 лет;
в) 30 лет;
г) 40 лет.

44. Как часто органы государственной власти должны пересматривать перечни сведений, подлежащих засекречиванию?
а) каждые 3 года;
б) каждые 5 лет;

в) каждые 7 лет;
г) каждые 10 лет.

45. Что из перечисленного является основанием для рассекречивания сведений, составляющих государственную тайну:
а) отсутствие в органах государственной власти Перечня сведений, составляющих государственную тайну;
б) принятие на себя обязательств перед государством по нераспространению сведений, составляющих государственную тайну;
в) *взятие на себя Россией обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;*
г) отсутствие специальных помещений для хранения документов, содержащих сведения, составляющие государственную тайну.

46. Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных:
а) осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник;
б) необходима в связи с осуществлением правосудия;
в) необходима в связи с выездом за пределы Российской Федерации;
г) необходима в соответствии с оперативно-розыскной деятельностью.

47. Режим документированной информации – это:
а) электронный документ с электронной подписью;
б) выделенная информация по определенной цели;
в) выделенная информация в любой знаковой форме;
г) электронная информация, позволяющая ее идентифицировать.

48. В правовой режим документированной информации входит:
а) государственная тайна;
б) банковская тайна;
в) персональные данные;
г) электронная цифровая подпись.

49. Засекречиванию подлежат сведения о:
а) фактах нарушения прав и свобод человека и гражданина;
б) состоянии демографии;
в) силах и средствах гражданской обороны;
г) состоянии преступности.

50. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:

а) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно;
б) для доставки почтовых отправлений;
в) в целях профессиональной деятельности журналиста;
г) в целях профессиональной деятельности оператора.

51. Открытость информации в архивных фондах обеспечивается:
а) различными режимами доступа к информации и переходом информации из одной категории доступа в другую;
б) различными режимами доступа к информации;
в) переходом информации из одной категории доступа в другую;
г) правовым статусом архивного фонда.

52. К государственной тайне не относятся сведения, защищаемые государством, распространение которых может нанести ущерб государству:
а) в экономической области;
б) в контрразведывательной деятельности;
в) в оперативно-разыскной деятельности;
г) о частной жизни политических деятелей.

53. Обработка персональных данных – это:
а) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
б) накопление, хранение и передача персональных данных;
в) размещение персональных данных в информационных системах;
г) только передача персональных данных.

54. Срок хранения персональных данных, осуществляемого в форме, позволяющей определить субъекта персональных данных:
а) 1 год;
б) 5 лет;
в) Не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено законом или договором;
г) 3 года.

55. Что такое коммерческая тайна?

а) сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

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

в) сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны;

г) защищаемая законом информация, доверенная или ставшая известной лицу (держателю информации) исключительно в силу исполнения им профессиональных обязанностей, не связанная с государственной или муниципальной службой.

56. Доктрина информационной безопасности не закрепляет следующие термины:

а) информация;

б) информационная безопасность Российской Федерации;

в) информационная угроза;

г) средства обеспечения информационной безопасности.

57. В соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» электронная подпись - это:

а) электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра;

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

в) информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;
г) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

58. В соответствии с Федеральным законом от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» к инсайдерской информации не относится:
а) информация о принятых решениях об итогах торгов (тендеров);
б) информация, полученная в ходе проводимых проверок, а также информация о результатах таких проверок;
в) информация о принятых решениях в отношении лиц, определенных ФЗ № 224, о выдаче, приостановлении действия или об аннулировании (отзыве) лицензий (разрешений, аккредитаций) на осуществление определенных видов деятельности, а также иных разрешений;
г) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

59. Каким нормативным правовым документом утвержден Порядок организации работы по обеспечению доступа к информации о деятельности Министерства внутренних дел Российской Федерации?
а) Приказом МВД России от 30 марта 2012 г. № 205;
б) Приказом МВД России от 14 марта 2012 года № 169;
в) Приказом МВД России от 27 октября 2015 г. № 1010;
г) Приказом МВД России от 24 декабря 2015 г. № 1228.

60. Каким нормативным правовым документом утверждены Правила организации доступа к информационно-телекоммуникационной сети Интернет в органах внутренних дел Российской Федерации?
а) Приказ МВД России от 30 марта 2012 г. № 205;
б) Приказ МВД России от 14 марта 2012 года № 169;
в) Приказ МВД России от 27 октября 2015 г. № 1010;
г) Приказ МВД России от 24 декабря 2015 г. N 1228.

61. Каким нормативным правовым документом утверждена Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года?
а) Приказом МВД России от 30 марта 2012 г. № 205;
б) Приказом МВД России от 14 марта 2012 года № 169;
в) Приказом МВД России от 27 октября 2015 г. № 1010;
г) Приказом МВД России от 24 декабря 2015 г. № 1228.

62. Каким нормативным правовым документом утвержден Перечень персональных данных, обрабатываемых в Министерстве внутренних дел Российской Федерации в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций?
а) Приказом МВД России от 29 декабря 2016 г. № 925;
б) Приказом МВД России от 14 марта 2012 года № 169;
в) Приказом МВД России от 27 октября 2015 г. № 1010;
г) Приказом МВД России от 24 декабря 2015 г. № 1228.

63. Каким ведомственным нормативным правовым документом утверждено Положение о Департаменте информационных технологий, связи и защиты информации МВД России?
а) Приказом МВД России от 16 июня 2011 г. № 681;
б) Приказом МВД России от 26 июля 2016 г. № 419;
в) Приказом МВД России от 19 января 2016 г. № 30
г) Приказом МВД России от 22 мая 2014 г. № 434.

64. Каким нормативным правовым документом утверждено Положение о Федеральной службе по техническому и экспортному контролю?
а) Приказом ФСТЭК России от 3 марта 2011 г. № 116;
б) Указом Президента Российской Федерации от 16 августа 2004 г. № 1085;
в) Федеральным законом от 18 июля 1999 г. № 183-ФЗ;
г) Постановлением Правительства Российской Федерации от 15 апреля 1995 г. № 333.

65. Каким нормативным правовым документом регламентированы вопросы защиты интеллектуальной собственности в Российской Федерации?
а) Законом РФ от 23.09.1992 N 3526-1 «О правовой охране топологий интегральных микросхем»;
б) *Гражданским кодексом Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ;*

в) Законом РФ от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах»;
г) Патентным законом Российской Федерации от 23.09.1992 № 3517-1.

66. Объектами авторского права не являются:
а) программы для электронных вычислительных машин (программы для ЭВМ);
б) литературные произведения;
в) изобретения;
г) аудиовизуальные произведения.

67. Объектами патентного права не являются:
а) программы для электронных вычислительных машин (программы для ЭВМ);
б) полезные модели;
в) промышленные образцы;
г) изобретения.

68. Каким нормативным правовым документом регламентированы вопросы государственной регистрации программ для ЭВМ и баз данных?
а) Законом РФ от 23.09.1992 № 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных»;
б) Гражданским кодексом Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ;
в) Законом РФ от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах»;
г) Патентным закон Российской Федерации от 23.09.1992 № 3517-1.

69. Какие элементы включает знак охраны авторского права:
а) латинская буква «С» в окружности, имя или наименование правообладателя, год первого опубликования произведения;
б) латинская буква «С» в окружности, имя или наименование автора, год первого опубликования произведения;
в) латинская буква «С» в окружности, псевдоним автора, год первого опубликования произведения;
г) латинская буква «С» в окружности, имя или наименование автора.

70. К показателям патентоспособности изобретения относятся:
а) новизна, наличие изобретательского уровня, промышленная применимость;
б) новизна, промышленная применимость;

в) возможность многократного воспроизведения образца путем производства соответствующего изделия, новизна, наличие изобретательского уровня, промышленная применимость;
г) возможность многократного воспроизведения образца путем производства соответствующего изделия, новизна, оригинальность, промышленная применимость.

71. Несут ли ответственность лица, виновные в нарушении норм, регулирующих обработку и защиту информации?
а) несут только дисциплинарную и уголовную ответственность;
б) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном действующим законодательством;
в) несут только дисциплинарную и административную ответственность;
г) не несут.

72. Какой вид ответственности наступает в случае совершения следующих действий: незаконное использование объектов авторского права или смежных прав, а равно приобретение, хранение, перевозка контрафактных экземпляров произведений или фонограмм в целях сбыта, совершенные в крупном размере?
а) административная ответственность;
б) уголовная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

73. Какой вид ответственности наступает в случае совершения следующих действий: ввоз, продажа, сдача в прокат или иное незаконное использование экземпляров произведений или фонограмм в целях извлечения дохода в случаях, если экземпляры произведений или фонограмм являются контрафактными в соответствии с законодательством Российской Федерации об авторском праве и смежных правах либо на экземплярах произведений или фонограмм указана ложная информация об их изготовителях, о местах их производства, а также об обладателях авторских и смежных прав, а равно иное нарушение авторских и смежных прав в целях извлечения дохода?
а) административная ответственность;
б) уголовная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

74. «Незаконное использование изобретения, полезной модели или промышленного образца, разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб» – это диспозиция:
а) ст.146 УК РФ;
б) ст.147 УК РФ;
в) ст.272 УК РФ;
г) ст. 7.12. КоАП РФ.

75. Какой вид ответственности предусмотрен действующим законодательством в случае нарушения условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)?
а) уголовная ответственность;
б) административная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

76. Какой вид ответственности предусмотрен действующим законодательством в случае использования несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)?
а) уголовная ответственность;
б) административная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

77. Какой вид ответственности предусмотрен действующим законодательством в случае занятия видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии?
а) уголовная ответственность;
б) административная ответственность;
в) дисциплинарная ответственность;
г) гражданско-правовая ответственность.

78. Общественно опасными последствиями в соответствии со ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» являются:
а) уничтожение компьютерной информации;
б) модификация либо копирование компьютерной информации;
в) блокирование компьютерной информации;
г) все вышеперечисленное.

79. Какой ущерб признается крупным в статьях главы 28 УК РФ «Преступления в сфере компьютерной информации»:
а) ущерб, сумма которого превышает пятьсот тыс. рублей;
б) ущерб, сумма которого превышает один миллион рублей;
в) ущерб, сумма которого превышает два миллиона рублей;
г) ущерб, сумма которого превышает сто тыс. рублей.

80. В каких формах выражается государственная измена в соответствии со ст. 275 УК РФ?
а) государственная измена в форме шпионажа;
б) государственная измена в форме выдачи государственной тайны;
в) государственная измена в форме оказания помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности против России;
г) все вышеперечисленное.

81. Допускается ли освобождение от уголовной ответственности лица, совершившего преступления, предусмотренные ст. ст. 275, 276?
а) нет, не допускается;
б) допускается, если оно своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации;
в) допускается, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации и если в его действиях не содержится иного состава преступления;
г) допускается, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба интересам Российской Федерации.

82. Кто является субъектом преступления, предусмотренного ст. 276 УК РФ?
а) гражданин РФ;
б) иностранный гражданин или лицо без гражданства;
в) государственный служащий;

г) лицо, которому государственная тайна была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации.

83. Какой вид ответственности предусмотрен действующим законодательством в случае получения сведений, составляющих государственную тайну, путем похищения, обмана, шантажа, принуждения, угрозы применения насилия либо иным незаконным способом?

а) уголовная ответственность;

б) административная ответственность;

в) дисциплинарная ответственность;

г) гражданско-правовая ответственность.

84. В соответствии с Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне» государственная тайна – это:

а) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

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

в) информация, основанная на документах, фактах;

г) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

85. В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для ИСПДн устанавливается:
а) два уровня защищенности персональных данных;
б) три уровня защищенности персональных данных;
в) четыре уровня защищенности персональных данных;
г) пять уровней защищенности персональных данных.

86. При проведении контроля за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах персональных данных регуляторы:
а) вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных;
б) не вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных;
в) вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных, только в установленных законом случаях;
г) не вправе ознакамливаться с персональными данными, обрабатываемыми в информационных системах персональных данных во всех случаях.

87. На какой орган исполнительной власти РФ возлагается функция уполномоченного органа по защите прав субъектов персональных данных?
а) Федеральную службу охраны Российской Федерации (ФСО России);
б) Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);
в) Федеральную службу безопасности Российской Федерации (ФСБ России);
г) Федеральную службу по техническому и экспортному контролю (ФСТЭК России).

88. Какой орган исполнительной власти РФ осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации?
а) ФСБ России;
б) МВД России;
в) ФСО России;
г) ФСТЭК России.

89. Что является организационной формой защиты информации?

а) разработка и реализация специальных законов, нормативных правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;
б) *регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;*
в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения;
г) формирование правового статуса всех субъектов в системе информационной безопасности и определение их ответственности за обеспечение информационной безопасности.

90. Что является правовой формой защиты информации?
а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;
б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;
в) оценка эффективности функционирования системы защиты информации;
г) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения.

91. Что является инженерно-технической формой защиты информации?
а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;
б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;
в) контроль выполнения установленных правил работы с защищаемой информацией;
г) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения.

92. Какой из перечисленных видов деятельности не подлежит обязательному лицензированию?
а) деятельность, связанная с защитой государственной тайны;
б) работа со сведениями, составляющими конфиденциальную информацию;
в) разработка и производство средств защиты конфиденциальной информации;
г) деятельность по технической защите конфиденциальной информации.

ЛИТЕРАТУРА

1. Всеобщая декларация прав человека: [принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.] // Рос. газета. - 1998. - 10 декабря (№ 245). – С. 3.
2. Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21 сентября 1970 г., 20 декабря 1971 г., 1 января 1990 г., 6 ноября 1990 г., 11 мая 1994 г.) // Бюллетень международных договоров. - март 2001 г. - №3.
3. Директива 95/46/ЕС Европейского Парламента и Совета от 24 октября 1995 г. «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (Принята в г. Люксембурге 24.10.1995, с изм. и доп. от 29.09.2003 г.). – Официальный Журнал Европейского Союза. – L 281. – 23.11.1995. – p. 31.
4. Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изм. и доп. от 21 сентября 1970 г., 20 декабря 1971 г., 1 января 1990 г., 6 ноября 1990 г., 11 мая 1994 г.) // Бюллетень международных договоров. - март 2001 г. - №3.
5. Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 г.
6. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) // Ведомости Верховного Совета СССР. - 1976 г. - №17(1831). - Ст. 291.
7. Директива Европейского парламента и Совета Европейского союза от 24 октября 1995 года № 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных» (в редакции Регламента Европейского парламента и Совета Европейского союза от 29 сентября 2003 г. № 1882/2003) [Электронный ресурс] - Режим доступа. - URL: http://online.zakon.kz/Document/ (дата обращения: 11.09.2019).
8. Конституция Российской Федерации (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 05 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ) // Собр. законодательства Рос. Федерации. – 2014. – № 31. – Ст. 4398.
9. Гражданский Кодекс Российской Федерации. Часть первая: Федеральный закон от 30.11.1994 № 51-ФЗ // Собр. законодательства РФ. 1994. № 32. Ст. 3301.
10. Семейный кодекс Российской Федерации от 29 декабря 1995 г. № 223-ФЗ // Собрание законодательства Российской Федерации от 1 января 1996 г. № 1 ст. 16.
11. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации - 17 июня 1996 г. - № 25 - Ст. 2954.

12. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. - 7 января 2002 г. - №1. - Ст. 1.
13. О безопасности : федеральный закон от 28.12.2010 № 390-ФЗ // СПС «КонсультантПлюс». [Электронный ресурс].
14. О государственной тайне: федеральный закон Российской Федерации от 21.07.1993 № 5485-1 (ред. от 18 июля 2009) // Собрание законодательства РФ. - 1997. - № 2.
15. О федеральной службе безопасности: федеральный закон от 3 апреля 1995 г. № 40-ФЗ // СЗ РФ. -1995. -№ 15. - Ст. 1269.
16. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 года № 149-ФЗ // СЗ РФ. 2006. -№31-1 ч. - ст. 3448.
17. Об исполнительном производстве: федеральный закон от 2 октября 2007 г. № 229-ФЗ// Собрание законодательства Российской Федерации от 8 октября 2007 г. - № 41 - ст. 4849.
18. Об информации, информатизации и защите информации: федеральный закон от 20 февраля 1995 г. № 24-ФЗ (утратил силу) // СЗ РФ. – 1995. - № 8 ст. 609.
19. О ратификации Конвенции Совета Европы о защите физических лиц при автоматической обработке персональных данных: федеральный закон от 19.12.2005 № 160-ФЗ // Москва, Кремль;19 декабря 2005 г. № 160-ФЗ.
20. О подготовке и проведении в Российской Федерации чемпионата мира по футболу FIFA 2018 года, Кубка конфедераций FIFA 2017 года и внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 07.06.2013 № 108-ФЗ (ред. от 29.12.2017)// Собрание законодательства РФ. - 10.06.2013. - № 23. - ст. 2866.
21. О стандартизации в Российской Федерации: федеральный закон от 29.06.2015 № 162-ФЗ
22. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 г. № 149-ФЗ // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.
23. О персональных данных: федеральный закон от 27 июля 2006 года № 152-ФЗ // СЗ РФ. 2006. - № 31 (1 ч.) - ст. 3451.
24. О коммерческой тайне: федеральный закон от 29 июля 2004 года № 98-ФЗ // Собрание законодательства РФ. - 2004. - №32.
25. О бухгалтерском учете: федеральный закон от 21 ноября 1996 г. № 129 // Собрание законодательства Российской Федерации. - 1996 г. - № 48. - Ст. 5369.
26. О банках и банковской деятельности: федеральный закон от 2 декабря 1990 г. № 395-1 (в ред. от 08.04.2008 № 46-ФЗ, с изм. от 27.10.2008 № 175-ФЗ) // СЗ РФ. 05.02.1996. № 6. Ст. 492; Российская газета. 1996. 10 февраля. № 27.

27. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: федеральный закон от 7 августа 2001 г. № 115-ФЗ // Собрание законодательства Российской Федерации. - 13 августа 2001 г. - №33 (Часть I). - Ст. 3418.
28. Об основах охраны здоровья граждан в Российской Федерации: федеральный закон от 21.11.2011 г. № 323-ФЗ (ред. от 23.07.2013 г.) // Собрание законодательства РФ. - 2011. - № 48. - ст. 6724.
29. О физической культуре и спорте в РФ: федеральный закон от 04 декабря 2007 № 329-ФЗ (ред. от 27 июля 2010) // Российская газета. - 2007. - 08 декабря. - № 276.
30. Об адвокатской деятельности и адвокатуре в Российской Федерации: федеральный закон от 31 мая 2002 г. № 63-ФЗ // Собрание законодательства Российской Федерации. - 2002г. - №23. - Ст.2102.
31. О свободе совести и о религиозных объединениях: федеральный закон от 26.09.1997 № 125-ФЗ (ред. от 02.07.2013) // Собрание законодательства РФ. 1997. № 39. Ст. 4465; 2013. № 27. Ст. 3477.
32. Об организации страхового дела в Российской Федерации: федеральный закон РФ от 27 ноября 1992 г. № 4015-1 // Российская газета. - 1993. - 12 января.
33. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г. №187-ФЗ // Собр. законодательства Рос. Федерации. - 2017. - № 31. - Части I-II. - Ст. 4736.
34. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. — 1997.-№ 10-ст. 1127.
35. Указ Президента Российской Федерации от 30 ноября 1995 года № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» // СЗ РФ. 1995. - № 49 - ст. 4775.
36. Об утверждении перечня сведений конфиденциального характера: Указ Президента РФ от 06.03.1997 № 188 // Собрание законодательства РФ. - 1997. - № 10. - Ст. 1127.
37. Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации».
38. Доктрина информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. №646 // Российская газета – 2016. – 6 дек.
39. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : постановление Правительства РФ от 08 февраля 2018 г. № 127 (ред. от 13 апреля 2019 г.) // Собр. законодательства Рос. Федерации. - 2018. - № 8. - Ст. 1204.

40. Постановление Правительства РФ от 6 июня 2008 г. № 440 «О внесении изменения в Постановление Правительства Российской Федерации от 18 сентября 2006 г. № 573» // СЗ РФ. 2008. - № 23 - ст. 2727.
41. Постановление Правительства РФ от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» // СЗ РФ. 1995. № 37. Ст. 3619.
42. Постановление Правительства РФ от 06.02.2010 № 63 (ред. от 29.12.2016) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне». Собрание законодательства РФ, 15.02.2010, № 7, ст. 762.
43. Постановление Правительства РФ от 22.08.1998 № 1003 «Об утверждении положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне» // Собрание законодательства РФ», 31.08.1998, № 35, ст. 4407
44. Постановление Правительства РФ от 6 июня 2008 г. № 440 «О внесении изменения в Постановление Правительства Российской Федерации от 18 сентября 2006 г. № 573» // СЗ РФ. 2008. - № 23 - ст. 2727.
45. Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации : постановление Правительства РФ от 15.09.2008 № 687 // Российская газета. 2008. 24 сентября.
46. Постановлении Правительства РФ от 21 марта 2012 г. № 211// СЗ РФ. 2012. № 45 ст. 6257.
47. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ.2012. № 45. ст. 6257.
48. Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // Собрание законодательства РФ, 23.03.2009, № 12, ст. 1431.
49. Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
50. Распоряжение Президента РФ от 16 апреля 2005 г. № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» // СЗ РФ. 2005. - № 17 - ст. 1547.
51. Об утверждении перечня медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, порядка получения и формы справки об отсутствии медицинских

противопоказаний для работы с использований сведений, составляющих государственную тайну : приказ Минздравсоцразвития РФ от 26.08.2011 № 989н (Зарегистрировано в Минюсте РФ 11.10.2011 № 22016) // Российская газета. 2011. № 234.
52. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» // Утверждена Заместителем директора ФСТЭК России, 15 февраля 2008 г.
53. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» // Утверждена Заместителем директора ФСТЭК России, 15 февраля 2008 г.
54. 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 14.11.2011 г. № 312 (ред. от 24.11.2014) // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2012. - № 9. – 27 февр.
55. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России от 25 декабря 2017 г. № 239
56. О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 : Приказ ФСТЭК России от 26 марта 2019 г. № 60
57. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006). (Дата введения 2008-02-01)
58. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с.
59. Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / С.Я. Казанцев, [и др.]; под ред. С.Я. Казанцева. – М.: Издательский центр «Академия», 2005. – 240 с.
60. Ожегов, С. И. Толковый словарь русского языка. 100 000 слов, терминов и выражений / С.И. Ожегов. - М.: Мир и Образование, 2015. - 759 с.
61. В. М. Глушков, [и др.] Энциклопедия кибернетики. //Киев, - 1975 .

62. С.Я. Казанцев, [и др.] Правовое обеспечение информационной безопасности: учеб. пособие для студ. высш. учеб. заведений / под ред. С.Я. Казанцева. – М.: Издательский центр «Академия», 2005. – 240 с.
63. Номоканон при Большом Требнике: его история и тексты, греческий и славянский, с объяснительными и критическими примечаниями : монография / А.С. Павлов. – Репр. изд. 1897 г. – Москва ; Берлин : Директ-Медиа, 2016. – 540 с.
64. Черданцев А.Ф., Кожевников С. Н. О понятии и содержании юридической ответственности // Правоведение. - 2001. - №5. - С. 29.
65. Чеботарева А.А. «Правовое обеспечение информационной безопасности личности в глобальном информационном обществе» // Диссертация на соискание ученой степени доктора юридических наук. Москва – 2017.
66. Чеботарева А.А. «Правовое обеспечение информационной безопасности личности в глобальном информационном обществе»: диссертация на соискание ученой степени доктора юридических наук: 12.00.13 – Чеботарева А.А. Москва – 2018. – 473 с.