**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ФЕДЕРАЛЬНЫЙ ЗАКОН**

**ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ**

**И О ЗАЩИТЕ ИНФОРМАЦИИ**

Принят

Государственной Думой

8 июля 2006 года

Одобрен

Советом Федерации

14 июля 2006 года

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.

(в ред. Федерального закона от 02.07.2013 N 187-ФЗ)

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

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

2) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

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

5) обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации - возможность получения информации и ее использования;

7) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

11.1) электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

(п. 11.1 введен Федеральным законом от 27.07.2010 N 227-ФЗ)

12) оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

13) сайт в сети "Интернет" - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет";

(п. 13 введен Федеральным законом от 28.07.2012 N 139-ФЗ, в ред. Федерального закона от 07.06.2013 N 112-ФЗ)

14) страница сайта в сети "Интернет" (далее также - интернет-страница) - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет";

(п. 14 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

15) доменное имя - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";

(п. 15 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

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

(п. 16 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

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

(п. 17 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

18) провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет";

(п. 18 введен Федеральным законом от 28.07.2012 N 139-ФЗ)

19) единая система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

(п. 19 введен Федеральным законом от 07.06.2013 N 112-ФЗ)

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

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.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. 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.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации

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

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 7. Общедоступная информация

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

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

4. Информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.

(часть 4 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

5. Информация в форме открытых данных размещается в сети "Интернет" с учетом требований законодательства Российской Федерации о государственной тайне. В случае, если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

(часть 5 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

6. В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда. В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных", размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

(часть 6 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

Статья 8. Право на доступ к информации

1. Граждане (физические лица) и организации (юридические лица) (далее - организации) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

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

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

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

(в ред. Федерального закона от 27.07.2010 N 227-ФЗ)

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

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

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации

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

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

КонсультантПлюс: примечание.

По вопросу, касающемуся порядка обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, см. Постановление Правительства РФ от 03.11.1994 N 1233.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 10. Распространение информации или предоставление информации

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

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

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

(введена Федеральным законом от 05.05.2014 N 97-ФЗ)

1. Организатором распространения информации в сети "Интернет" является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет".

2. Организатор распространения информации в сети "Интернет" обязан в установленном Правительством Российской Федерации порядке уведомить федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления деятельности, указанной в части 1 настоящей статьи.

3. Организатор распространения информации в сети "Интернет" обязан хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети "Интернет" и информацию об этих пользователях в течение шести месяцев с момента окончания осуществления таких действий, а также предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

4. Организатор распространения информации в сети "Интернет" обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий. Порядок взаимодействия организаторов распространения информации в сети "Интернет" с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, устанавливается Правительством Российской Федерации.

5. Обязанности, предусмотренные настоящей статьей, не распространяются на операторов государственных информационных систем, операторов муниципальных информационных систем, операторов связи, оказывающих услуги связи на основании соответствующей лицензии, в части лицензируемой деятельности, а также не распространяются на граждан (физических лиц), осуществляющих указанную в части 1 настоящей статьи деятельность для личных, семейных и домашних нужд. Правительством Российской Федерации в целях применения положений настоящей статьи определяется перечень личных, семейных и домашних нужд при осуществлении деятельности, указанной в части 1 настоящей статьи.

6. Состав информации, подлежащей хранению в соответствии с частью 3 настоящей статьи, место и правила ее хранения, порядок ее предоставления уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, а также порядок осуществления контроля за деятельностью организаторов распространения информации в сети "Интернет", связанной с хранением такой информации, и федеральный орган исполнительной власти, уполномоченный на осуществление этого контроля, определяются Правительством Российской Федерации.

Статья 10.2. Особенности распространения блогером общедоступной информации

(введена Федеральным законом от 05.05.2014 N 97-ФЗ)

1. Владелец сайта и (или) страницы сайта в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет" (далее - блогер), при размещении и использовании указанной информации, в том числе при размещении указанной информации на данных сайте или странице сайта иными пользователями сети "Интернет", обязан обеспечивать соблюдение законодательства Российской Федерации, в частности:

1) не допускать использование сайта или страницы сайта в сети "Интернет" в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) проверять достоверность размещаемой общедоступной информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию;

3) не допускать распространение информации о частной жизни гражданина с нарушением гражданского законодательства;

4) соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;

5) соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации;

6) соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций.

2. При размещении информации на сайте или странице сайта в сети "Интернет" не допускается:

1) использование сайта или страницы сайта в сети "Интернет" в целях сокрытия или фальсификации общественно значимых сведений, распространения заведомо недостоверной информации под видом достоверных сообщений;

2) распространение информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями.

3. Блогер имеет право:

1) свободно искать, получать, передавать и распространять информацию любым способом в соответствии с законодательством Российской Федерации;

2) излагать на своих сайте или странице сайта в сети "Интернет" свои личные суждения и оценки с указанием своего имени или псевдонима;

3) размещать или допускать размещение на своих сайте или странице сайта в сети "Интернет" текстов и (или) иных материалов других пользователей сети "Интернет", если размещение таких текстов и (или) иных материалов не противоречит законодательству Российской Федерации;

4) распространять на возмездной основе рекламу в соответствии с гражданским законодательством, Федеральным законом от 13 марта 2006 года N 38-ФЗ "О рекламе" на своих сайте или странице сайта в сети "Интернет".

4. Злоупотребление правом на распространение общедоступной информации, выразившееся в нарушении требований частей 1, 2 и 3 настоящей статьи, влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.

5. Блогер обязан разместить на своих сайте или странице сайта в сети "Интернет" свои фамилию и инициалы, электронный адрес для направления ему юридически значимых сообщений.

6. Блогер обязан разместить на своих сайте или странице сайта в сети "Интернет" незамедлительно при получении решение суда, вступившее в законную силу и содержащее требование о его опубликовании на данных сайте или странице сайта.

7. Владельцы сайтов в сети "Интернет", которые зарегистрированы в соответствии с Законом Российской Федерации от 27 декабря 1991 года N 2124-1 "О средствах массовой информации" в качестве сетевых изданий, не являются блогерами.

8. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет". В целях обеспечения формирования реестра сайтов и (или) страниц сайтов в сети "Интернет" федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) организует мониторинг сайтов и страниц сайтов в сети "Интернет";

2) утверждает методику определения количества пользователей сайта или страницы сайта в сети "Интернет" в сутки;

3) вправе запрашивать у организаторов распространения информации в сети "Интернет", блогеров и иных лиц информацию, необходимую для ведения такого реестра. Указанные лица обязаны предоставлять запрашиваемую информацию не позднее чем в течение десяти дней со дня получения запроса федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", сайтов или страниц сайтов, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет", включая рассмотрение соответствующих обращений граждан или организаций, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) включает указанные сайт или страницу сайта в сети "Интернет" в реестр сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет";

2) определяет провайдера хостинга или иное обеспечивающее размещение сайта или страницы сайта в сети "Интернет" лицо;

3) направляет провайдеру хостинга или указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать блогера;

4) фиксирует дату и время направления уведомления провайдеру хостинга или указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

10. В течение трех рабочих дней с момента получения уведомления, указанного в пункте 3 части 9 настоящей статьи, провайдер хостинга или указанное в пункте 2 части 9 настоящей статьи лицо обязаны предоставить данные, позволяющие идентифицировать блогера.

11. После получения данных, указанных в пункте 3 части 9 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет блогеру уведомление о включении его сайта или страницы сайта в реестр сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет", с указанием требований законодательства Российской Федерации, применимых к данным сайту или странице сайта в сети "Интернет".

12. В случае, если доступ к сайту или странице сайта в сети "Интернет" на протяжении трех месяцев составляет в течение суток менее трех тысяч пользователей сети "Интернет", данный сайт или данная страница сайта в сети "Интернет" по заявлению блогера исключается из реестра сайтов и (или) страниц сайтов в сети "Интернет", на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети "Интернет", о чем блогеру направляется соответствующее уведомление. Данные сайт или страница сайта в сети "Интернет" могут быть исключены из этого реестра при отсутствии заявления блогера, если доступ к данным сайту или странице сайта в сети "Интернет" на протяжении шести месяцев составляет в течение суток менее трех тысяч пользователей сети "Интернет".

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

3. Утратил силу. - Федеральный закон от 06.04.2011 N 65-ФЗ.

КонсультантПлюс: примечание.

В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

(в ред. Федерального закона от 06.04.2011 N 65-ФЗ)

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети "Интернет" и иных подобных информационно-телекоммуникационных сетей;

4) обеспечение информационной безопасности детей.

(п. 4 введен Федеральным законом от 21.07.2011 N 252-ФЗ)

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 13. Информационные системы

1. Информационные системы включают в себя:

1) 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;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы. В случаях и в порядке, установленных федеральными законами, оператор информационной системы должен обеспечить возможность размещения информации в сети "Интернет" в форме открытых данных.

(в ред. Федерального закона от 07.06.2013 N 112-ФЗ)

3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.

6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

Статья 14. Государственные информационные системы

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд.

(часть 2 в ред. Федерального закона от 28.12.2013 N 396-ФЗ)

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления - Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае, если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьей 14 Федерального закона от 9 февраля 2009 года N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления", государственные информационные системы должны обеспечивать размещение такой информации в сети "Интернет" в форме открытых данных.

(в ред. Федерального закона от 07.06.2013 N 112-ФЗ)

4.1. Правительство Российской Федерации определяет случаи, при которых доступ с использованием сети "Интернет" к информации, содержащейся в государственных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе идентификации и аутентификации, а также порядок использования единой системы идентификации и аутентификации.

(часть 4.1 введена Федеральным законом от 07.06.2013 N 112-ФЗ)

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

6. Правительство Российской Федерации вправе устанавливать требования к порядку создания и ввода в эксплуатацию отдельных государственных информационных систем.

(в ред. Федерального закона от 28.12.2013 N 396-ФЗ)

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

(в ред. Федерального закона от 27.07.2010 N 227-ФЗ)

Статья 15. Использование информационно-телекоммуникационных сетей

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено

(введена Федеральным законом от 28.07.2012 N 139-ФЗ)

1. В целях ограничения доступа к сайтам в сети "Интернет", содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система "Единый реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (далее - реестр).

2. В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети "Интернет", содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено.

3. Создание, формирование и ведение реестра осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра оператора реестра - организацию, зарегистрированную на территории Российской Федерации.

5. Основаниями для включения в реестр сведений, указанных в части 2 настоящей статьи, являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети "Интернет":

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

(пп. "г" введен Федеральным законом от 05.04.2013 N 50-ФЗ)

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" и Федерального закона от 11 ноября 2003 года N 138-ФЗ "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети "Интернет" и иных средств связи;

(пп. "д" введен Федеральным законом от 21.07.2014 N 222-ФЗ)

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети "Интернет", информацией, распространение которой в Российской Федерации запрещено.

6. Решение о включении в реестр доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено, может быть обжаловано владельцем сайта в сети "Интернет", провайдером хостинга, оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", в суд в течение трех месяцев со дня принятия такого решения.

7. В течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети "Интернет" в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети "Интернет" и уведомить его о необходимости незамедлительного удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.

8. В течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети "Интернет" в реестр владелец сайта в сети "Интернет" обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети "Интернет" провайдер хостинга обязан ограничить доступ к такому сайту в сети "Интернет" в течение суток.

9. В случае непринятия провайдером хостинга и (или) владельцем сайта в сети "Интернет" мер, указанных в частях 7 и 8 настоящей статьи, сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, включается в реестр.

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет", содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к такому сайту в сети "Интернет".

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра исключает из реестра доменное имя, указатель страницы сайта в сети "Интернет" или сетевой адрес, позволяющий идентифицировать сайт в сети "Интернет", на основании обращения владельца сайта в сети "Интернет", провайдера хостинга или оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", не позднее чем в течение трех дней со дня такого обращения после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено, либо на основании вступившего в законную силу решения суда об отмене решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о включении в реестр доменного имени, указателя страницы сайта в сети "Интернет" или сетевого адреса, позволяющего идентифицировать сайт в сети "Интернет".

12. Порядок взаимодействия оператора реестра с провайдером хостинга и порядок получения доступа к содержащейся в реестре информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

13. Порядок ограничения доступа к сайтам в сети "Интернет", предусмотренный настоящей статьей, не применяется к информации, порядок ограничения доступа к которой предусмотрен статьей 15.3 настоящего Федерального закона.

(часть 13 введена Федеральным законом от 28.12.2013 N 398-ФЗ)

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

(введена Федеральным законом от 02.07.2013 N 187-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", фильмов, в том числе кинофильмов, телефильмов, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие фильмы или информацию, на основании вступившего в силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней:

1) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети "Интернет", указанного информационного ресурса, обслуживающего владельца сайта в сети "Интернет", на котором размещена информация, содержащая фильмы, в том числе кинофильмы, телефильмы, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания;

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении исключительных прав на фильмы, в том числе кинофильмы, телефильмы, с указанием наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети "Интернет", на котором размещена информация, содержащая фильмы, в том числе кинофильмы, телефильмы, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания, а также указателей страниц сайта в сети "Интернет", позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в соответствующей информационной системе.

3. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить незаконно размещенную информацию и (или) принять меры по ограничению доступа к ней.

4. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 2 настоящей статьи лица уведомления о необходимости удалить незаконно размещенную информацию владелец информационного ресурса обязан удалить такую информацию. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи.

5. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 2 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 3 и 4 настоящей статьи, доменное имя сайта в сети "Интернет", его сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать информацию, содержащую фильмы, в том числе кинофильмы, телефильмы, или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, и размещенную без разрешения правообладателя или иного законного основания, а также иные сведения об этом сайте и информация направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети "Интернет", или к размещенной на нем информации.

6. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней со дня получения судебного акта об отмене ограничения доступа к информационному ресурсу, содержащему фильмы, в том числе кинофильмы, телефильмы, или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без разрешения правообладателя или иного законного основания, уведомляет провайдера хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо и операторов связи об отмене мер по ограничению доступа к данному информационному ресурсу.

7. В течение суток с момента получения по системе взаимодействия сведений об информационном ресурсе, содержащем фильмы, в том числе кинофильмы, телефильмы, или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без разрешения правообладателя или иного законного основания, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к такому информационному ресурсу, в том числе к сайту в сети "Интернет", или к странице сайта.

8. Порядок функционирования информационной системы взаимодействия устанавливается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. Предусмотренный настоящей статьей порядок не применяется к информации, подлежащей включению в реестр в соответствии со статьей 15.1 настоящего Федерального закона.

Статья 15.3. Порядок ограничения доступа к информации, распространяемой с нарушением закона

(введена Федеральным законом от 28.12.2013 N 398-ФЗ)

1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи, незамедлительно:

1) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, в том числе к сайту в сети "Интернет", или к информации, размещенной на нем и содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка. Данное требование должно содержать доменное имя сайта в сети "Интернет", сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать такую информацию;

2) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети "Интернет", указанного информационного ресурса, обслуживающего владельца сайта в сети "Интернет", на котором размещена информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка;

3) направляет провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети "Интернет", на котором размещена информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, а также указателей страниц сайта в сети "Интернет", позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

4) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

3. После получения по системе взаимодействия требования федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети "Интернет", или к информации, размещенной на нем и содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

4. В течение суток с момента получения уведомления, указанного в пункте 3 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 2 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

5. В случае, если владелец информационного ресурса удалил информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

6. После получения уведомления, указанного в части 5 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан незамедлительно уведомить по системе взаимодействия оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", о возобновлении доступа к информационному ресурсу, в том числе к сайту в сети "Интернет".

7. После получения уведомления, указанного в части 6 настоящей статьи, оператор связи незамедлительно возобновляет доступ к информационному ресурсу, в том числе к сайту в сети "Интернет".

Статья 15.4. Порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети "Интернет"

(введена Федеральным законом от 05.05.2014 N 97-ФЗ)

1. В случае установленного вступившим в законную силу постановлением по делу об административном правонарушении неисполнения организатором распространения информации в сети "Интернет" обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, в его адрес (адрес его филиала или представительства) уполномоченным федеральным органом исполнительной власти направляется уведомление, в котором указывается срок исполнения таких обязанностей, составляющий не менее чем пятнадцать дней.

2. В случае неисполнения организатором распространения информации в сети "Интернет" в указанный в уведомлении срок обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, доступ к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет" и функционирование которых обеспечивается данным организатором, до исполнения таких обязанностей ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети "Интернет", на основании вступившего в законную силу решения суда или решения уполномоченного федерального органа исполнительной власти.

3. Порядок взаимодействия уполномоченного федерального органа исполнительной власти с организатором распространения информации в сети "Интернет", порядок направления указанного в части 1 настоящей статьи уведомления, порядок ограничения и возобновления доступа к указанным в части 2 настоящей статьи информационным системам и (или) программам и порядок информирования граждан (физических лиц) о таком ограничении устанавливаются Правительством Российской Федерации.

КонсультантПлюс: примечание.

В соответствии с Федеральным законом от 21.07.2014 N 242-ФЗ с 1 сентября 2015 года данный документ будет дополнен статьей 15.5.

Статья 16. Защита информации

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

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

КонсультантПлюс: примечание.

В соответствии с Федеральным законом от 21.07.2014 N 242-ФЗ с 1 сентября 2015 года часть 4 статьи 16 будет дополнена пунктом 7 следующего содержания:

"7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.".

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

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

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

4. Провайдер хостинга и владелец сайта в сети "Интернет" не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.

(часть 4 введена Федеральным законом от 02.07.2013 N 187-ФЗ)

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

1) Федеральный закон от 20 февраля 1995 года N 24-ФЗ "Об информации, информатизации и защите информации" (Собрание законодательства Российской Федерации, 1995, N 8, ст. 609);

2) Федеральный закон от 4 июля 1996 года N 85-ФЗ "Об участии в международном информационном обмене" (Собрание законодательства Российской Федерации, 1996, N 28, ст. 3347);

3) статью 16 Федерального закона от 10 января 2003 года N 15-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2003, N 2, ст. 167);

4) статью 21 Федерального закона от 30 июня 2003 года N 86-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской Федерации, 2003, N 27, ст. 2700);

5) статью 39 Федерального закона от 29 июня 2004 года N 58-ФЗ "О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления" (Собрание законодательства Российской Федерации, 2004, N 27, ст. 2711).

Президент

Российской Федерации

В.ПУТИН

Москва, Кремль

27 июля 2006 года

N 149-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ  
  
ФЕДЕРАЛЬНЫЙ ЗАКОН  
  
О ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ,  
ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ

Принят

Государственной Думой

21 декабря 2010 года

Одобрен

Советом Федерации

24 декабря 2010 года

Список изменяющих документов

(см. [Обзор](http://www.consultant.ru/document/cons_doc_LAW_133757/?dst=100009) изменений данного документа)

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.

2. Настоящий Федеральный закон не распространяется на отношения в сфере:

1) оборота информационной продукции, содержащей научную, научно-техническую, статистическую информацию;

2) распространения информации, недопустимость ограничения доступа к которой установлена Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_165971/) от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и другими федеральными законами;

3) оборота информационной продукции, имеющей значительную историческую, художественную или иную культурную ценность для общества;

4) рекламы.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

1) доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации;

2) знак информационной продукции - графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информационной продукции, предусмотренной [частью 3 статьи 6](http://www.consultant.ru/document/cons_doc_LAW_169775/?frame=1#p107) настоящего Федерального закона;

3) зрелищное мероприятие - демонстрация информационной продукции в месте, доступном для детей, и в месте, где присутствует значительное число лиц, не принадлежащих к обычному кругу семьи, в том числе посредством проведения театрально-зрелищных, культурно-просветительных и зрелищно-развлекательных мероприятий;

4) информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;

5) информационная продукция - предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети "Интернет", и сетей подвижной радиотелефонной связи;

(в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_169766/?dst=100011) от 28.07.2012 N 139-ФЗ)

(см. текст в предыдущей [редакции](http://www.consultant.ru/document/cons_doc_LAW_108808/?dst=100022))

6) информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;

7) информация, причиняющая вред здоровью и (или) развитию детей, - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом;

8) информация порнографического характера - информация, представляемая в виде натуралистических изображения или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного;

9) классификация информационной продукции - распределение информационной продукции в зависимости от ее тематики, жанра, содержания и художественного оформления по возрастным категориям детей в порядке, установленном настоящим Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_169775/?frame=1#p96);

10) места, доступные для детей, - общественные места, доступ ребенка в которые и (или) нахождение ребенка в которых не запрещены, в том числе общественные места, в которых ребенок имеет доступ к продукции средств массовой информации и (или) размещаемой в информационно-телекоммуникационных сетях информационной продукции;

11) натуралистические изображение или описание - изображение или описание в любой форме и с использованием любых средств человека, животного, отдельных частей тела человека и (или) животного, действия (бездействия), события, явления, их последствий с фиксированием внимания на деталях, анатомических подробностях и (или) физиологических процессах;

12) оборот информационной продукции - предоставление и (или) распространение информационной продукции, включая ее продажу (в том числе распространение по подписке), аренду, прокат, раздачу, выдачу из фондов общедоступных библиотек, публичный показ, публичное исполнение (в том числе посредством зрелищных мероприятий), распространение посредством эфирного или кабельного вещания, информационно-телекоммуникационных сетей, в том числе сети "Интернет", и сетей подвижной радиотелефонной связи;

(в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_169766/?dst=100012) от 28.07.2012 N 139-ФЗ)

(см. текст в предыдущей [редакции](http://www.consultant.ru/document/cons_doc_LAW_108808/?dst=100029))

13) эксперт - лицо, отвечающее требованиям настоящего Федерального закона и привлекаемое для проведения экспертизы информационной продукции и дачи экспертного заключения или осуществления классификации информационной продукции и проведения ее экспертизы.

Статья 3. Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию

Законодательство Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, состоит из [Конституции](http://www.consultant.ru/document/cons_doc_LAW_2875/) Российской Федерации, настоящего Федерального закона, других федеральных законов и принимаемых в соответствии с ними иных нормативных правовых актов.

Статья 4. Полномочия федерального органа исполнительной власти, органов государственной власти субъектов Российской Федерации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию

1. К полномочиям федерального органа исполнительной власти, уполномоченного Правительством Российской Федерации, в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, относятся:

1) разработка и реализация единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию;

2) разработка и реализация федеральных целевых программ обеспечения информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции;

3) установление [порядка](http://www.consultant.ru/document/cons_doc_LAW_136850/?dst=100010) проведения экспертизы информационной продукции, предусмотренной настоящим Федеральным законом;

4) государственный надзор за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

(в ред. Федеральных законов от 28.07.2012 [N 139-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_169766/?dst=100013), от 14.10.2014 [N 307-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_169745/?dst=100768))

(см. текст в предыдущей [редакции](http://www.consultant.ru/document/cons_doc_LAW_148988/?dst=3))

2. К полномочиям органов государственной власти субъектов Российской Федерации в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, относятся разработка и реализация региональных программ обеспечения информационной безопасности детей, производства информационной продукции для детей и оборота информационной продукции.

Статья 5. Виды информации, причиняющей вред здоровью и (или) развитию детей

1. К информации, причиняющей вред здоровью и (или) развитию детей, относится:

1) информация, предусмотренная [частью 2](http://www.consultant.ru/document/cons_doc_LAW_169775/#p78) настоящей статьи и запрещенная для распространения среди детей;

2) информация, которая предусмотрена [частью 3](http://www.consultant.ru/document/cons_doc_LAW_169775/#p90) настоящей статьи с учетом положений [статей 7](http://www.consultant.ru/document/cons_doc_LAW_169775/?frame=1#p125) - [10](http://www.consultant.ru/document/cons_doc_LAW_169775/?frame=1#p143) настоящего Федерального закона и распространение которой среди детей определенных возрастных категорий ограничено.

2. К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

(в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_148269/?dst=100009) от 29.06.2013 N 135-ФЗ)

(см. текст в предыдущей [редакции](http://www.consultant.ru/document/cons_doc_LAW_144690/?dst=100048))

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

(п. 8 введен Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_144630/?dst=100032) от 05.04.2013 N 50-ФЗ)

3. К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

1) представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2) вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 16 июня 2014 г. N 161 г. Москва

"Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию"

**Зарегистрирован в Минюсте РФ 12 августа 2014 г.**

**Регистрационный N 33555**

В соответствии с частью 3 статьи 11 Федерального закона от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (Собрание законодательства Российской Федерации, 2011, N 1, ст. 48; 2012, N 31, ст. 4328; 2013, N 14, ст. 1658; N 26, ст. 3208; N 27, ст. 3477) и подпунктом 5.2.25[14] Положения о Министерстве связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. N 418 (Собрание законодательства Российской Федерации, 2008, N 23, ст. 2708; N 42, ст. 4825; N 46, ст. 5337; 2009, N 3, ст. 378; N 6, ст. 738; N 33, ст. 4088; 2010, N 13, ст. 1502; N 26, ст. 3350; N 30, ст. 4099; N 31, ст. 4251; 2011, N 3, ст. 542; N 2, ст. 338; N 6, ст. 888; N 14, ст. 1935; N 21, ст. 2965; N 44, ст. 6272; N 49, ст. 7283; 2012, N 20, ст. 2540; N 37, ст. 5001; N 39, ст. 5270; N 46, ст. 6347; 2013, N 13, ст. 1568; N 33, ст. 4386; N 45, ст. 5822), **приказываю**:

1. Утвердить прилагаемые требования к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

**Министр Н. Никифоров**

**Требования к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию**

**I. Общие положения**

1. Требования к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию (далее - Требования), применяются при обороте информационной продукции, содержащей информацию, запрещенную для распространения среди детей в соответствии с частью 2 статьи 5 Федерального закона от 29 декабря 2010 г. N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (Собрание законодательства Российской Федерации, 2011, N 1, ст. 48; 2012, N 31, ст. 4328; 2013, N 14, ст. 1658; N 26, ст. 3208; N 27, ст. 3477) (далее - Федеральный закон N 436-ФЗ), в местах, доступных для детей (далее - оборот информационной продукции, запрещенной для детей; информация, запрещенная для распространения среди детей), а также при предоставлении в соответствии с частью 1 статьи 14 Федерального закона N 436-ФЗ доступа к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети "Интернет", в местах, доступных для детей (далее - предоставление доступа к информации; сеть "Интернет").

2. Требования не распространяются на операторов связи, оказывающих услуги связи, предусматривающие предоставление доступа к информации, распространяемой посредством сети "Интернет", на основании договоров об оказании услуг связи, заключенных в письменной форме.

**II. Административные**

и организационные меры защиты детей от информации, причиняющей вред

их здоровью и (или) развитию

3. К административным мерам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, относятся следующие.

3.1. Издание локальных актов, определяющих:

3.1.1. Процедуры присвоения и размещения знака информационной продукции и (или) текстового предупреждения об информационной продукции, запрещенной для детей, в соответствии со статьями 11 - 14 Федерального закона N 436-ФЗ;

3.1.2. Условия присутствия в соответствии с законодательством Российской Федерации детей на публичном показе, при публичном исполнении, демонстрации посредством зрелищного мероприятия информационной продукции, запрещенной для детей, в случае их организации и (или) проведения;

3.1.3. Дополнительные требования к обороту информационной продукции, запрещенной для детей, и ее фрагментов, распространяемых посредством эфирного и кабельного, теле- и радиовещания, сети "Интернет" и сетей подвижной радиотелефонной связи, в местах доступных для детей в соответствии со статьями 13, 14 и 16 Федерального закона N 436-ФЗ;

3.1.4. Меры защиты детей от информации, причиняющей вред их здоровью и (или) развитию, направленные на повышение осведомленности лиц, находящихся в месте оборота информационной продукции, запрещенной для детей, о необходимости обеспечения информационной безопасности детей и защиты детей от информации, причиняющей вред их здоровью и (или) развитию;

3.1.5. Процедуры, направленные на предотвращение, выявление и устранение нарушений законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию;

3.2. Ознакомление работников, в трудовые обязанности которых входит организация и осуществление оборота информационной продукции, запрещенной для детей, с положениями законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, с локальными актами, изданными в соответствии с подпунктом 3.1 Требований;

3.3. Назначение работника, ответственного за применение административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, учитывающих специфику оборота информационной продукции, запрещенной для детей, и за проверку порядка их применения;

3.4. Осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствием применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, локальным актам, изданным в соответствии с подпунктом 3.1 Требований, и предусматривающего:

3.4.1. Рассмотрение в срок, не превышающий десяти рабочих дней со дня получения, обращений, жалоб или претензий о нарушениях законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, включая несоответствие применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, Требованиям, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, и направление мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий;

3.4.2. Установление в течение десяти рабочих дней со дня получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, причин и условий возникновения такого доступа и принятие мер по их устранению.

4. К организационным мерам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, относятся следующие.

4.1. Размещение на информационных стендах в местах, доступных для детей, а также доведение иным доступным способом до третьих лиц сведений об изданных в соответствии с подпунктом 3.1 Требований локальных актах;

4.2. Размещение на официальном сайте производителя и (или) распространителя, осуществляющих оборот информационной продукции, запрещенной для детей, в сети "Интернет" локальных актов, изданных в соответствии с подпунктом 3.1 Требований, а также сведений о применении административных и организационных мер, и обеспечение возможности свободного доступа к указанным документам.

**III. Технические и программно-аппаратные средства защиты детей** **от информации, причиняющей вред их здоровью и (или) развитию**

5. К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяемым при предоставлении доступа к информации, распространяемой посредством сети "Интернет", относятся следующие.

5.1. Средства ограничения доступа к техническим средствам доступа к сети "Интернет";

5.2. Средства ограничения доступа к сети "Интернет" с технических средств третьих лиц;

5.3. Средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах в сети "Интернет".

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ФЕДЕРАЛЬНЫЙ ЗАКОН**

**О ПЕРСОНАЛЬНЫХ ДАННЫХ**

Принят

Государственной Думой

8 июля 2006 года

Одобрен

Советом Федерации

14 июля 2006 года

|  |
| --- |
| Список изменяющих документов |

(в ред. Федеральных законов от 25.11.2009 N 266-ФЗ,

от 27.12.2009 N 363-ФЗ, от 28.06.2010 N 123-ФЗ, от 27.07.2010 N 204-ФЗ,

от 27.07.2010 N 227-ФЗ, от 29.11.2010 N 313-ФЗ от 23.12.2010 N 359-ФЗ,

от 04.06.2011 N 123-ФЗ, от 25.07.2011 N 261-ФЗ, от 05.04.2013 N 43-ФЗ,

от 23.07.2013 N 205-ФЗ, от 21.12.2013 N 363-ФЗ, от 04.06.2014 N 142-ФЗ,

от 21.07.2014 N 216-ФЗ, от 21.07.2014 N 242-ФЗ, от 03.07.2016 N 231-ФЗ,

от 22.02.2017 N 16-ФЗ, от 01.07.2017 N 148-ФЗ, от 29.07.2017 N 223-ФЗ,

от 31.12.2017 N 498-ФЗ)

**Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ**

**Статья 1. Сфера действия настоящего Федерального закона**

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

(часть 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Действие настоящего Федерального закона не распространяется на отношения, возникающие при:

1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;

5) утратил силу. - Федеральный закон от 29.07.2017 N 223-ФЗ.

3. Предоставление, распространение, передача и получение информации о деятельности судов в Российской Федерации, содержащей персональные данные, ведение и использование информационных систем и информационно-телекоммуникационных сетей в целях создания условий для доступа к указанной информации осуществляются в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации".

(часть 3 введена Федеральным законом от 29.07.2017 N 223-ФЗ)

**Статья 2. Цель настоящего Федерального закона**

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

**Статья 3. Основные понятия, используемые в настоящем Федеральном законе**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

В целях настоящего Федерального закона используются следующие основные понятия:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

3) обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Статья 4. Законодательство Российской Федерации в области персональных данных**

1. Законодательство Российской Федерации в области персональных данных основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из настоящего Федерального закона и других определяющих случаи и особенности обработки персональных данных федеральных законов.

2. На основании и во исполнение федеральных законов государственные органы, Банк России, органы местного самоуправления в пределах своих полномочий могут принимать нормативные правовые акты, нормативные акты, правовые акты (далее - нормативные правовые акты) по отдельным вопросам, касающимся обработки персональных данных. Такие акты не могут содержать положения, ограничивающие права субъектов персональных данных, устанавливающие не предусмотренные федеральными законами ограничения деятельности операторов или возлагающие на операторов не предусмотренные федеральными законами обязанности, и подлежат официальному опубликованию.

(часть 2 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

3. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации, могут быть установлены федеральными законами и иными нормативными правовыми актами Российской Федерации с учетом положений настоящего Федерального закона.

4. Если международным договором Российской Федерации установлены иные правила, чем те, которые предусмотрены настоящим Федеральным законом, применяются правила международного договора.

**Глава 2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**Статья 5. Принципы обработки персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

**Статья 6. Условия обработки персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных настоящим Федеральным законом. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

(п. 3 в ред. Федерального закона от 29.07.2017 N 223-ФЗ)

3.1) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

(п. 3.1 введен Федеральным законом от 29.07.2017 N 223-ФЗ)

4) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

(в ред. Федерального закона от 05.04.2013 N 43-ФЗ)

5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

(в ред. Федеральных законов от 21.12.2013 N 363-ФЗ, от 03.07.2016 N 231-ФЗ)

6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом "О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон "О микрофинансовой деятельности и микрофинансовых организациях", либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

(в ред. Федерального закона от 03.07.2016 N 231-ФЗ)

8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

10) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

1.1. Обработка персональных данных объектов государственной охраны и членов их семей осуществляется с учетом особенностей, предусмотренных Федеральным законом от 27 мая 1996 года N 57-ФЗ "О государственной охране".

(часть 1.1 введена Федеральным законом от 01.07.2017 N 148-ФЗ)

2. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 настоящего Федерального закона.

3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона.

4. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

5. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

**Статья 7. Конфиденциальность персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

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

**Статья 8. Общедоступные источники персональных данных**

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

**Статья 9. Согласие субъекта персональных данных на обработку его персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

3. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона, возлагается на оператора.

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

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона.

**Статья 10. Специальные категории персональных данных**

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка указанных в части 1 настоящей статьи специальных категорий персональных данных допускается в случаях, если:

1) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2) персональные данные сделаны общедоступными субъектом персональных данных;

(п. 2 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

(п. 2.1 введен Федеральным законом от 25.11.2009 N 266-ФЗ)

2.2) обработка персональных данных осуществляется в соответствии с Федеральным законом от 25 января 2002 года N 8-ФЗ "О Всероссийской переписи населения";

(п. 2.2 введен Федеральным законом от 27.07.2010 N 204-ФЗ)

2.3) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

(п. 2.3 введен Федеральным законом от 25.07.2011 N 261-ФЗ, в ред. Федерального закона от 21.07.2014 N 216-ФЗ)

3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

(п. 3 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4) обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

5) обработка персональных данных членов (участников) общественного объединения или религиозной организации осуществляется соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

6) обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

(п. 6 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

(п. 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7.1) обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

(п. 7.1 введен Федеральным законом от 23.07.2013 N 205-ФЗ)

8) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

(п. 8 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

9) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации, государственными органами, муниципальными органами или организациями в целях устройства детей, оставшихся без попечения родителей, на воспитание в семьи граждан;

(п. 9 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

10) обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

(п. 10 введен Федеральным законом от 04.06.2014 N 142-ФЗ)

3. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

4. Обработка специальных категорий персональных данных, осуществлявшаяся в случаях, предусмотренных частями 2 и 3 настоящей статьи, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

**Статья 11. Биометрические персональные данные**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

(в ред. Федеральных законов от 04.06.2014 N 142-ФЗ, от 31.12.2017 N 498-ФЗ)

**Статья 12. Трансграничная передача персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

**Статья 13. Особенности обработки персональных данных в государственных или муниципальных информационных системах персональных данных**

1. Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

2. Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.

3. Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных. Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

4. В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

**Глава 3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ**

**Статья 14. Право субъекта персональных данных на доступ к его персональным данным**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

4. В случае, если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

**Статья 15. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации**

1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено.

2. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных, указанную в части 1 настоящей статьи.

**Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных**

1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

4. Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

**Статья 17. Право на обжалование действий или бездействия оператора**

1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

**Глава 4. ОБЯЗАННОСТИ ОПЕРАТОРА**

**Статья 18. Обязанности оператора при сборе персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 настоящего Федерального закона.

2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 настоящей статьи, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные настоящим Федеральным законом права субъекта персональных данных;

5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 настоящей статьи, в случаях, если:

1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;

5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона.

(часть 5 введена Федеральным законом от 21.07.2014 N 242-ФЗ)

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

(введена Федеральным законом от 25.07.2011 N 261-ФЗ)

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами.

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

**Статья 19. Меры по обеспечению безопасности персональных данных при их обработке**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. Состав и содержание необходимых для выполнения установленных Правительством Российской Федерации в соответствии с частью 3 настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

КонсультантПлюс: примечание.

По вопросу разработки нормативных правовых актов, определяющих угрозы безопасности персональных данных, см. Методические рекомендации, утв. ФСБ России 31.03.2015 N 149/7/2/6-432.

5. Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

6. Наряду с угрозами безопасности персональных данных, определенных в нормативных правовых актах, принятых в соответствии с частью 5 настоящей статьи, ассоциации, союзы и иные объединения операторов своими решениями вправе определить дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с учетом содержания персональных данных, характера и способов их обработки.

7. Проекты нормативных правовых актов, указанных в части 5 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Проекты решений, указанных в части 6 настоящей статьи, подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в порядке, установленном Правительством Российской Федерации. Решение федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, об отказе в согласовании проектов решений, указанных в части 6 настоящей статьи, должно быть мотивированным.

8. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при обработке персональных данных в государственных информационных системах персональных данных осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

9. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, решением Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных могут быть наделены полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии с настоящей статьей, при их обработке в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных, без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

10. Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11. Для целей настоящей статьи под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

**Статья 20. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. Оператор обязан сообщить в порядке, предусмотренном статьей 14 настоящего Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 настоящего Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

4. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

**Статья 21. Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных**

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5 настоящей статьи, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

**Статья 22. Уведомление об обработке персональных данных**

1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

(п. 1 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

4) сделанных субъектом персональных данных общедоступными;

(п. 4 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

(п. 9 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

3. Уведомление, предусмотренное частью 1 настоящей статьи, направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление должно содержать следующие сведения:

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

1) наименование (фамилия, имя, отчество), адрес оператора;

2) цель обработки персональных данных;

3) категории персональных данных;

4) категории субъектов, персональные данные которых обрабатываются;

5) правовое основание обработки персональных данных;

6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;

7) описание мер, предусмотренных статьями 18.1 и 19 настоящего Федерального закона, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

(п. 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

7.1) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

(п. 7.1 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

8) дата начала обработки персональных данных;

9) срок или условие прекращения обработки персональных данных;

10) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

(п. 10 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

10.1) сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

(п. 10.1 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

11) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

(п. 11 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

4. Уполномоченный орган по защите прав субъектов персональных данных в течение тридцати дней с даты поступления уведомления об обработке персональных данных вносит сведения, указанные в части 3 настоящей статьи, а также сведения о дате направления указанного уведомления в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

5. На оператора не могут возлагаться расходы в связи с рассмотрением уведомления об обработке персональных данных уполномоченным органом по защите прав субъектов персональных данных, а также в связи с внесением сведений в реестр операторов.

6. В случае предоставления неполных или недостоверных сведений, указанных в части 3 настоящей статьи, уполномоченный орган по защите прав субъектов персональных данных вправе требовать от оператора уточнения предоставленных сведений до их внесения в реестр операторов.

7. В случае изменения сведений, указанных в части 3 настоящей статьи, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

(часть 7 в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

**Статья 22.1. Лица, ответственные за организацию обработки персональных данных в организациях**

(введена Федеральным законом от 25.07.2011 N 261-ФЗ)

1. Оператор, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных.

2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся оператором, и подотчетно ему.

3. Оператор обязан предоставлять лицу, ответственному за организацию обработки персональных данных, сведения, указанные в части 3 статьи 22 настоящего Федерального закона.

4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

**Глава 5. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ И НАДЗОР ЗА ОБРАБОТКОЙ**

**ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ**

**ТРЕБОВАНИЙ НАСТОЯЩЕГО ФЕДЕРАЛЬНОГО ЗАКОНА**

(в ред. Федерального закона от 22.02.2017 N 16-ФЗ)

**Статья 23. Уполномоченный орган по защите прав субъектов персональных данных**

1. Уполномоченным органом по защите прав субъектов персональных данных является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

(часть 1 в ред. Федерального закона от 22.02.2017 N 16-ФЗ)

1.1. Уполномоченный орган по защите прав субъектов персональных данных обеспечивает, организует и осуществляет государственный контроль и надзор за соответствием обработки персональных данных требованиям настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов (государственный контроль и надзор за обработкой персональных данных). Порядок организации и проведения проверок юридических лиц и индивидуальных предпринимателей, являющихся операторами, уполномоченным органом по защите прав субъектов персональных данных, а также порядок организации и осуществления государственного контроля и надзора за обработкой персональных данных иными лицами, являющимися операторами, устанавливается Правительством Российской Федерации.

(часть 1.1 введена Федеральным законом от 22.02.2017 N 16-ФЗ)

2. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

3. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

1) запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

2) осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации;

(п. 3.1 введен Федеральным законом от 21.07.2014 N 242-ФЗ)

4) принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований настоящего Федерального закона;

5) обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов персональных данных в суде;

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

5.1) направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 настоящего Федерального закона;

(п. 5.1 введен Федеральным законом от 25.07.2011 N 261-ФЗ)

6) направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

7) направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;

8) вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;

9) привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

4. В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

5. Уполномоченный орган по защите прав субъектов персональных данных обязан:

1) организовывать в соответствии с требованиями настоящего Федерального закона и других федеральных законов защиту прав субъектов персональных данных;

2) рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой персональных данных, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;

3) вести реестр операторов;

4) осуществлять меры, направленные на совершенствование защиты прав субъектов персональных данных;

5) принимать в установленном законодательством Российской Федерации порядке по представлению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, федерального органа исполнительной власти в области государственной охраны или федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, меры по приостановлению или прекращению обработки персональных данных;

(в ред. Федерального закона от 01.07.2017 N 148-ФЗ)

6) информировать государственные органы, а также субъектов персональных данных по их обращениям или запросам о положении дел в области защиты прав субъектов персональных данных;

7) выполнять иные предусмотренные законодательством Российской Федерации обязанности.

5.1. Уполномоченный орган по защите прав субъектов персональных данных осуществляет сотрудничество с органами, уполномоченными по защите прав субъектов персональных данных в иностранных государствах, в частности международный обмен информацией о защите прав субъектов персональных данных, утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

(часть 5.1 введена Федеральным законом от 25.07.2011 N 261-ФЗ)

6. Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

7. Уполномоченный орган по защите прав субъектов персональных данных ежегодно направляет отчет о своей деятельности Президенту Российской Федерации, в Правительство Российской Федерации и Федеральное Собрание Российской Федерации. Указанный отчет подлежит опубликованию в средствах массовой информации.

8. Финансирование уполномоченного органа по защите прав субъектов персональных данных осуществляется за счет средств федерального бюджета.

9. При уполномоченном органе по защите прав субъектов персональных данных создается на общественных началах консультативный совет, порядок формирования и порядок деятельности которого определяются уполномоченным органом по защите прав субъектов персональных данных.

**Статья 24. Ответственность за нарушение требований настоящего Федерального закона**

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

(часть 2 введена Федеральным законом от 25.07.2011 N 261-ФЗ)

**Глава 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

**Статья 25. Заключительные положения**

1. Настоящий Федеральный закон вступает в силу по истечении ста восьмидесяти дней после дня его официального опубликования.

2. После дня вступления в силу настоящего Федерального закона обработка персональных данных, включенных в информационные системы персональных данных до дня его вступления в силу, осуществляется в соответствии с настоящим Федеральным законом.

2.1. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пунктах 5, 7.1, 10 и 11 части 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2013 года.

(часть 2.1 введена Федеральным законом от 25.07.2011 N 261-ФЗ)

3. Утратил силу. - Федеральный закон от 25.07.2011 N 261-ФЗ.

4. Операторы, которые осуществляют обработку персональных данных до дня вступления в силу настоящего Федерального закона и продолжают осуществлять такую обработку после дня его вступления в силу, обязаны направить в уполномоченный орган по защите прав субъектов персональных данных, за исключением случаев, предусмотренных частью 2 статьи 22 настоящего Федерального закона, уведомление, предусмотренное частью 3 статьи 22 настоящего Федерального закона, не позднее 1 января 2008 года.

5. Отношения, связанные с обработкой персональных данных, осуществляемой государственными органами, юридическими лицами, физическими лицами при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в субъекте Российской Федерации - городе федерального значения Москве, регулируются настоящим Федеральным законом, если иное не предусмотрено Федеральным законом "Об особенностях регулирования отдельных правоотношений в связи с присоединением к субъекту Российской Федерации - городу федерального значения Москве территорий и о внесении изменений в отдельные законодательные акты Российской Федерации".

(часть 5 введена Федеральным законом от 05.04.2013 N 43-ФЗ)

Президент

Российской Федерации

В.ПУТИН

Москва, Кремль

27 июля 2006 года

N 152-ФЗ

**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**ФЕДЕРАЛЬНЫЙ ЗАКОН**

**О БЕЗОПАСНОСТИ**

Принят

Государственной Думой

7 декабря 2010 года

Одобрен

Советом Федерации

15 декабря 2010 года

|  |
| --- |
| Список изменяющих документов |

(в ред. Федерального закона от 05.10.2015 N 285-ФЗ)

**Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ**

**Статья 1. Предмет регулирования настоящего Федерального закона**

Настоящий Федеральный закон определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее - безопасность, национальная безопасность), полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации (далее - Совет Безопасности).

**Статья 2. Основные принципы обеспечения безопасности**

Основными принципами обеспечения безопасности являются:

1) соблюдение и защита прав и свобод человека и гражданина;

2) законность;

3) 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;

4) приоритет предупредительных мер в целях обеспечения безопасности;

5) 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.

**Статья 3. Содержание деятельности по обеспечению безопасности**

Деятельность по обеспечению безопасности включает в себя:

1) прогнозирование, выявление, анализ и оценку угроз безопасности;

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

3) правовое регулирование в области обеспечения безопасности;

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

5) применение специальных экономических мер в целях обеспечения безопасности;

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

7) организацию научной деятельности в области обеспечения безопасности;

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

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

10) международное сотрудничество в целях обеспечения безопасности;

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

**Статья 4. Государственная политика в области обеспечения безопасности**

1. 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.

2. Основные направления государственной политики в области обеспечения безопасности определяет Президент Российской Федерации.

3. Государственная политика в области обеспечения безопасности реализуется федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления на основе стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов, разрабатываемых Советом Безопасности и утверждаемых Президентом Российской Федерации.

4. Граждане и общественные объединения участвуют в реализации государственной политики в области обеспечения безопасности.

**Статья 5. Правовая основа обеспечения безопасности**

Правовую основу обеспечения безопасности составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, настоящий Федеральный закон, другие федеральные законы и иные нормативные правовые акты Российской Федерации, законы и иные нормативные правовые акты субъектов Российской Федерации, органов местного самоуправления, принятые в пределах их компетенции в области безопасности.

**Статья 6. Координация деятельности по обеспечению безопасности**

Координацию деятельности по обеспечению безопасности осуществляют Президент Российской Федерации и формируемый и возглавляемый им Совет Безопасности, а также в пределах своей компетенции Правительство Российской Федерации, федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления.

**Статья 7. Международное сотрудничество в области обеспечения безопасности**

1. Международное сотрудничество Российской Федерации в области обеспечения безопасности осуществляется на основе общепризнанных принципов и норм международного права и международных договоров Российской Федерации.

2. Основными целями международного сотрудничества в области обеспечения безопасности являются:

1) защита суверенитета и территориальной целостности Российской Федерации;

2) защита прав и законных интересов российских граждан за рубежом;

3) укрепление отношений со стратегическими партнерами Российской Федерации;

4) участие в деятельности международных организаций, занимающихся проблемами обеспечения безопасности;

5) развитие двусторонних и многосторонних отношений в целях выполнения задач обеспечения безопасности;

6) содействие урегулированию конфликтов, включая участие в миротворческой деятельности.

**Глава 2. ПОЛНОМОЧИЯ ФЕДЕРАЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ**

**ВЛАСТИ, ФУНКЦИИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ СУБЪЕКТОВ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ И ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ**

**В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ**

**Статья 8. Полномочия Президента Российской Федерации в области обеспечения безопасности**

Президент Российской Федерации:

1) определяет основные направления государственной политики в области обеспечения безопасности;

2) утверждает стратегию национальной безопасности Российской Федерации, иные концептуальные и доктринальные документы в области обеспечения безопасности;

3) формирует и возглавляет Совет Безопасности;

4) устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых он осуществляет;

5) в порядке, установленном Федеральным конституционным законом от 30 мая 2001 года N 3-ФКЗ "О чрезвычайном положении", вводит на территории Российской Федерации или в отдельных ее местностях чрезвычайное положение, осуществляет полномочия в области обеспечения режима чрезвычайного положения;

6) принимает в соответствии с законодательством Российской Федерации:

а) решение о применении специальных экономических мер в целях обеспечения безопасности;

б) меры по защите граждан от преступных и иных противоправных действий, по противодействию терроризму и экстремизму;

7) решает в соответствии с законодательством Российской Федерации вопросы, связанные с обеспечением защиты:

а) информации и государственной тайны;

б) населения и территорий от чрезвычайных ситуаций;

8) осуществляет иные полномочия в области обеспечения безопасности, возложенные на него Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

**Статья 9. Полномочия палат Федерального Собрания Российской Федерации в области обеспечения безопасности**

1. Совет Федерации Федерального Собрания Российской Федерации:

1) рассматривает принятые Государственной Думой Федерального Собрания Российской Федерации федеральные законы в области обеспечения безопасности;

2) утверждает указ Президента Российской Федерации о введении чрезвычайного положения.

2. Государственная Дума Федерального Собрания Российской Федерации принимает федеральные законы в области обеспечения безопасности.

**Статья 10. Полномочия Правительства Российской Федерации в области обеспечения безопасности**

Правительство Российской Федерации:

1) участвует в определении основных направлений государственной политики в области обеспечения безопасности;

2) формирует федеральные целевые программы в области обеспечения безопасности и обеспечивает их реализацию;

3) устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых оно осуществляет;

4) организует обеспечение федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления средствами и ресурсами, необходимыми для выполнения задач в области обеспечения безопасности;

5) осуществляет иные полномочия в области обеспечения безопасности, возложенные на него Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами и нормативными правовыми актами Президента Российской Федерации.

**Статья 11. Полномочия федеральных органов исполнительной власти в области обеспечения безопасности**

Федеральные органы исполнительной власти выполняют задачи в области обеспечения безопасности в соответствии с Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, нормативными правовыми актами Президента Российской Федерации и нормативными правовыми актами Правительства Российской Федерации.

**Статья 12. Функции органов государственной власти субъектов Российской Федерации и органов местного самоуправления в области обеспечения безопасности**

Органы государственной власти субъектов Российской Федерации и органы местного самоуправления в пределах своей компетенции обеспечивают исполнение законодательства Российской Федерации в области обеспечения безопасности.

**Глава 3. СТАТУС СОВЕТА БЕЗОПАСНОСТИ**

**Статья 13. Совет Безопасности**

1. Совет Безопасности является конституционным совещательным органом, осуществляющим подготовку решений Президента Российской Федерации по вопросам обеспечения безопасности, организации обороны, военного строительства, оборонного производства, военно-технического сотрудничества Российской Федерации с иностранными государствами, по иным вопросам, связанным с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также по вопросам международного сотрудничества в области обеспечения безопасности.

2. Совет Безопасности формируется и возглавляется Президентом Российской Федерации.

3. Положение о Совете Безопасности Российской Федерации утверждается Президентом Российской Федерации.

4. В целях реализации задач и функций Совета Безопасности Президентом Российской Федерации могут создаваться рабочие органы Совета Безопасности и аппарат Совета Безопасности.

**Статья 14. Основные задачи и функции Совета Безопасности**

1. Основными задачами Совета Безопасности являются:

1) обеспечение условий для осуществления Президентом Российской Федерации полномочий в области обеспечения безопасности;

2) формирование государственной политики в области обеспечения безопасности и контроль за ее реализацией;

3) прогнозирование, выявление, анализ и оценка угроз безопасности, оценка военной опасности и военной угрозы, выработка мер по их нейтрализации;

4) подготовка предложений Президенту Российской Федерации:

а) о мерах по предупреждению и ликвидации чрезвычайных ситуаций и преодолению их последствий;

б) о применении специальных экономических мер в целях обеспечения безопасности;

в) о введении, продлении и об отмене чрезвычайного положения;

5) координация деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации принятых Президентом Российской Федерации решений в области обеспечения безопасности;

6) оценка эффективности деятельности федеральных органов исполнительной власти в области обеспечения безопасности.

2. Основными функциями Совета Безопасности являются:

1) рассмотрение вопросов обеспечения безопасности, организации обороны, военного строительства, оборонного производства, военно-технического сотрудничества Российской Федерации с иностранными государствами, иных вопросов, связанных с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также вопросов международного сотрудничества в области обеспечения безопасности;

2) анализ информации о реализации основных направлений государственной политики в области обеспечения безопасности, о социально-политической и об экономической ситуации в стране, о соблюдении прав и свобод человека и гражданина;

3) разработка и уточнение стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов, а также критериев и показателей обеспечения национальной безопасности;

4) осуществление стратегического планирования в области обеспечения безопасности;

5) рассмотрение проектов законодательных и иных нормативных правовых актов Российской Федерации по вопросам, отнесенным к ведению Совета Безопасности;

6) подготовка проектов нормативных правовых актов Президента Российской Федерации по вопросам обеспечения безопасности и осуществления контроля деятельности федеральных органов исполнительной власти в области обеспечения безопасности;

7) организация работы по подготовке федеральных программ в области обеспечения безопасности и осуществление контроля за их реализацией;

8) организация научных исследований по вопросам, отнесенным к ведению Совета Безопасности.

3. Президент Российской Федерации может возложить на Совет Безопасности иные задачи и функции в соответствии с законодательством Российской Федерации.

**Статья 15. Состав Совета Безопасности**

1. В состав Совета Безопасности входят Председатель Совета Безопасности Российской Федерации, которым по должности является Президент Российской Федерации; Секретарь Совета Безопасности Российской Федерации (далее - Секретарь Совета Безопасности); постоянные члены Совета Безопасности и члены Совета Безопасности.

2. Постоянные члены Совета Безопасности входят в состав Совета Безопасности по должности в порядке, определяемом Президентом Российской Федерации. Секретарь Совета Безопасности входит в число постоянных членов Совета Безопасности.

3. Члены Совета Безопасности назначаются Президентом Российской Федерации в порядке, им определяемом.

4. Члены Совета Безопасности принимают участие в заседаниях Совета Безопасности с правом совещательного голоса.

5. Секретарем Совета Безопасности, постоянными членами Совета Безопасности и членами Совета Безопасности могут быть граждане Российской Федерации, не имеющие гражданства иностранного государства либо вида на жительство или иного документа, подтверждающего право на постоянное проживание гражданина Российской Федерации на территории иностранного государства.

**Статья 16. Секретарь Совета Безопасности**

1. Секретарь Совета Безопасности является должностным лицом, обеспечивающим реализацию возложенных на Совет Безопасности задач и функций.

2. Секретарь Совета Безопасности назначается на должность и освобождается от должности Президентом Российской Федерации, которому подчиняется непосредственно.

3. Полномочия Секретаря Совета Безопасности определяются Президентом Российской Федерации.

4. Секретарь Совета Безопасности обязан сообщать в порядке, предусмотренном указами Президента Российской Федерации, о возникновении личной заинтересованности при исполнении должностных обязанностей, которая приводит или может привести к конфликту интересов, а также принимать меры по предотвращению или урегулированию такого конфликта.

(часть 4 введена Федеральным законом от 05.10.2015 N 285-ФЗ)

**Статья 17. Организация деятельности Совета Безопасности**

1. Деятельность Совета Безопасности осуществляется в форме заседаний и совещаний.

2. Порядок организации и проведения заседаний и совещаний Совета Безопасности определяется Президентом Российской Федерации.

**Статья 18. Решения Совета Безопасности**

1. Решения Совета Безопасности принимаются на его заседаниях и совещаниях постоянными членами Совета Безопасности в порядке, определяемом Президентом Российской Федерации. Постоянные члены Совета Безопасности обладают равными правами при принятии решений.

2. Решения Совета Безопасности вступают в силу после их утверждения Президентом Российской Федерации.

3. Вступившие в силу решения Совета Безопасности обязательны для исполнения государственными органами и должностными лицами.

4. В целях реализации решений Совета Безопасности Президентом Российской Федерации могут издаваться указы и распоряжения.

**Глава 4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

**Статья 19. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации**

Признать утратившими силу:

1) Закон Российской Федерации от 5 марта 1992 года N 2446-1 "О безопасности" (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, N 15, ст. 769);

2) Постановление Верховного Совета Российской Федерации от 5 марта 1992 года N 2446/1-1 "О введении в действие Закона Российской Федерации "О безопасности" (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992, N 15, ст. 770);

3) Закон Российской Федерации от 25 декабря 1992 года N 4235-1 "О дополнении статьи 14 Закона Российской Федерации "О безопасности" (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, N 2, ст. 77);

4) Постановление Верховного Совета Российской Федерации от 25 декабря 1992 года N 4236-1 "О порядке введения в действие Закона Российской Федерации "О дополнении статьи 14 Закона Российской Федерации "О безопасности" (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, N 2, ст. 78);

5) статью 9 Федерального закона от 25 июля 2002 года N 116-ФЗ "О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с совершенствованием государственного управления в области пожарной безопасности" (Собрание законодательства Российской Федерации, 2002, N 30, ст. 3033);

6) статью 2 Федерального закона от 7 марта 2005 года N 15-ФЗ "О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательного акта Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления в сфере защиты и охраны Государственной границы Российской Федерации" (Собрание законодательства Российской Федерации, 2005, N 10, ст. 763);

7) статью 1 Федерального закона от 25 июля 2006 года N 128-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения требований к замещению государственных и муниципальных должностей" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3427);

8) статью 3 Федерального закона от 2 марта 2007 года N 24-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения требований к лицам, замещающим государственные или муниципальные должности, а также должности государственной или муниципальной службы" (Собрание законодательства Российской Федерации, 2007, N 10, ст. 1151);

9) статью 1 Федерального закона от 26 июня 2008 года N 103-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного управления в области таможенного дела" (Собрание законодательства Российской Федерации, 2008, N 26, ст. 3022).

**Статья 20. Вступление в силу настоящего Федерального закона**

Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Президент

Российской Федерации

Д.МЕДВЕДЕВ

Москва, Кремль

28 декабря 2010 года

N 390-ФЗ

Указ Президента РФ от 4 марта 2013 г. N 183  
"О рассмотрении общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса "Российская общественная инициатива"

#### С изменениями и дополнениями от:

В целях обеспечения развития и укрепления гражданского общества, защиты прав человека и гражданина, участия граждан в управлении делами государства постановляю:

1. Утвердить прилагаемые [Правила](http://ivo.garant.ru/#/document/70326884/entry/48) рассмотрения общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса "Российская общественная инициатива".

2. Установить, что рассмотрению в соответствии с [Правилами](http://ivo.garant.ru/#/document/70326884/entry/48), утвержденными настоящим Указом, подлежат направленные гражданами Российской Федерации с использованием интернет-ресурса "Российская общественная инициатива":

а) общественные инициативы, реализуемые на федеральном уровне, - с 15 апреля 2013 г.;

б) общественные инициативы, реализуемые на региональном и муниципальном уровнях, - с 1 ноября 2013 г.

[Указом](http://ivo.garant.ru/#/document/70681398/entry/1) Президента РФ от 23 июня 2014 г. N 452 Указ дополнен пунктом 2.1

2.1. Установить, что общественные инициативы, предусмотренные [пунктом 2](http://ivo.garant.ru/#/document/70326884/entry/4) настоящего Указа, могут быть направлены только гражданами Российской Федерации, лично предъявившими при регистрации в федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" основной документ, удостоверяющий личность гражданина Российской Федерации.

Не допускается голосование по таким общественным инициативам граждан Российской Федерации, не предъявивших при регистрации в указанной информационной системе основной документ, удостоверяющий личность гражданина Российской Федерации.

[Указом](http://ivo.garant.ru/#/document/70681398/entry/1) Президента РФ от 23 июня 2014 г. N 452 Указ дополнен пунктом 2.2

2.2. Установить, что ответственность за проверку основного документа и удостоверение личности гражданина Российской Федерации, регистрируемого в федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме", несут уполномоченные лица органов и организаций, осуществляющие регистрацию в указанной информационной системе.

3. Установить, что некоммерческой организацией, уполномоченной на осуществление функций, предусмотренных [Правилами](http://ivo.garant.ru/#/document/70326884/entry/48), утвержденными настоящим Указом, является Фонд развития информационной демократии и гражданского общества "Фонд информационной демократии".

4. Правительству Российской Федерации включить в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, интернет-ресурс "Российская общественная инициатива".

5. Правительству Российской Федерации, высшим должностным лицам (руководителям высших исполнительных органов государственной власти) субъектов Российской Федерации привести свои акты в соответствие с настоящим Указом.

6. Настоящий Указ вступает в силу со дня его подписания.

|  |  |
| --- | --- |
| Президент Российской Федерации | В. Путин |

Москва, Кремль

4 марта 2013 года

N 183

Правила  
рассмотрения общественных инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса "Российская общественная инициатива"  
(утв. [Указом](http://ivo.garant.ru/#/document/70326884/entry/0) Президента РФ от 4 марта 2013 г. N 183)

1. Общественными инициативами считаются предложения граждан Российской Федерации (далее - граждане) по вопросам социально-экономического развития страны, совершенствования государственного и муниципального управления, направленные с использованием интернет-ресурса "Российская общественная инициатива" (далее - интернет-ресурс) и отвечающие установленным настоящими Правилами требованиям.

2. Направлять общественные инициативы с использованием интернет-ресурса и голосовать за них могут граждане Российской Федерации, достигшие возраста 18 лет, зарегистрированные в федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

3. Размещению общественной инициативы на интернет-ресурсе предшествует обязательная предварительная экспертиза, за исключением случаев, установленных настоящими Правилами. Срок проведения предварительной экспертизы не должен превышать два месяца.

4. Функции по проведению предварительной экспертизы общественной инициативы, принятию решения о размещении общественной инициативы на интернет-ресурсе (в разделе для голосования) или об отказе в ее размещении, а также по обеспечению работы интернет-ресурса осуществляет уполномоченная некоммерческая организация.

5. Для реализации своих функций уполномоченная некоммерческая организация вправе запрашивать и получать сведения, необходимые материалы от федеральных органов государственной власти, федеральных государственных органов, органов государственной власти субъектов Российской Федерации и органов местного самоуправления.

6. Направление общественной инициативы осуществляется путем заполнения на русском языке специальной формы на интернет-ресурсе.

7. Текст общественной инициативы не должен содержать нецензурных либо оскорбительных выражений, угроз жизни или здоровью граждан, призывов к осуществлению экстремистской деятельности.

Общественная инициатива, в тексте которой содержатся нецензурные либо оскорбительные выражения, угрозы жизни или здоровью граждан, а также призывы к осуществлению экстремистской деятельности, снимается уполномоченной некоммерческой организацией с рассмотрения без проведения предварительной экспертизы, о чем гражданин, направивший такую инициативу, уведомляется в электронном виде.

8. Гражданин, направивший общественную инициативу, указывает, на каком уровне (федеральном, региональном или муниципальном), по его мнению, должна быть реализована данная инициатива.

9. Уполномоченная некоммерческая организация вправе принять решение о снятии общественной инициативы с рассмотрения без проведения предварительной экспертизы в случаях, если гражданином повторно направлена общественная инициатива, по которой было принято решение об отказе в ее размещении на интернет-ресурсе или которая не получила в ходе голосования необходимой поддержки, и при этом в общественной инициативе не приводятся новые доводы или не указываются новые обстоятельства, либо если аналогичная общественная инициатива уже размещена на интернет-ресурсе и получила необходимую поддержку в ходе голосования либо голосование по ней не завершено.

О данном решении гражданин, направивший общественную инициативу, уведомляется в электронном виде.

10. В ходе предварительной экспертизы устанавливаются соответствие общественной инициативы [Конституции](http://ivo.garant.ru/#/document/10103000/entry/0) Российской Федерации, общепризнанным принципам и нормам международного права, в том числе в области прав, свобод и законных интересов граждан, актуальность проблемы, содержащейся в общественной инициативе, обоснованность предлагаемых вариантов ее решения.

11. По результатам предварительной экспертизы уполномоченная некоммерческая организация принимает решение:

а) о размещении общественной инициативы на интернет-ресурсе (в разделе для голосования) и начале процедуры голосования;

б) об отказе в размещении общественной инициативы на интернет-ресурсе;

в) об изменении уровня реализации общественной инициативы.

12. О принятом по результатам предварительной экспертизы решении уполномоченная некоммерческая организация уведомляет гражданина, направившего общественную инициативу, в электронном виде. При этом уведомление об отказе в размещении общественной инициативы на интернет-ресурсе или об изменении уровня ее реализации должно быть мотивированным.

13. Уполномоченная некоммерческая организация принимает решение об отказе в размещении общественной инициативы на интернет-ресурсе в случаях, если:

а) общественная инициатива противоречит [Конституции](http://ivo.garant.ru/#/document/10103000/entry/0) Российской Федерации, общепризнанным принципам и нормам международного права, в том числе в области прав, свобод и законных интересов граждан;

б) общественная инициатива противоречит [статье 6](http://ivo.garant.ru/#/document/12135919/entry/6) Федерального конституционного закона от 28 июня 2004 г. N 5-ФКЗ "О референдуме Российской Федерации";

в) общественная инициатива не содержит описания проблемы, либо в общественной инициативе не предложены варианты решения проблемы, либо предлагаемые варианты не обоснованы.

14. Размещенная на интернет-ресурсе общественная инициатива должна получить необходимую поддержку в ходе голосования с использованием интернет-ресурса. Поддержанной считается инициатива, которая в течение одного года после ее размещения на интернет-ресурсе получила:

а) не менее 100 тыс. голосов граждан - в поддержку инициативы федерального уровня;

б) не менее 5 процентов голосов граждан, постоянно проживающих на территории соответствующего субъекта Российской Федерации (для субъектов Российской Федерации с численностью населения более 2 млн. человек - не менее 100 тыс. голосов граждан, постоянно проживающих на территории соответствующего субъекта Российской Федерации), - в поддержку инициативы регионального уровня;

в) не менее 5 процентов голосов граждан, постоянно проживающих на территории соответствующего муниципального образования, - в поддержку инициативы муниципального уровня.

15. Голосование по общественной инициативе с использованием интернет-ресурса начинается в день размещения этой инициативы на интернет-ресурсе (в разделе для голосования) и проводится в течение одного года.

16. Система голосования с использованием интернет-ресурса организуется по принципу "один человек - один голос" и предусматривает для граждан возможность проголосовать как за инициативу, так и против нее.

17. Уполномоченная некоммерческая организация обеспечивает:

а) возможность свободного использования гражданами интернет-ресурса для ознакомления с размещаемыми на нем общественными инициативами, итогами голосования, принятыми решениями, а также для получения информации о ходе и результатах реализации общественной инициативы;

б) возможность голосования, обработку голосов, поданных путем дистанционного электронного голосования, и достоверность его результатов.

18. Общественная инициатива, не получившая в ходе голосования необходимой поддержки, считается неподдержанной и снимается с рассмотрения. Информация об этом размещается на интернет-ресурсе.

19. Общественная инициатива, получившая в ходе голосования необходимую поддержку, направляется в электронном виде уполномоченной некоммерческой организацией в экспертную рабочую группу соответствующего уровня (федерального, регионального или муниципального) для проведения экспертизы и принятия решения о целесообразности разработки проекта соответствующего нормативного правового акта и (или) об иных мерах по реализации данной инициативы. Информация о направлении общественной инициативы в экспертную рабочую группу соответствующего уровня и принятых ею решениях размещается на интернет-ресурсе.

20. При направлении общественной инициативы в экспертную рабочую группу уполномоченная некоммерческая организация указывает следующую информацию:

а) содержание инициативы;

б) уровень реализации инициативы;

в) количество голосов, поданных за инициативу, и количество голосов, поданных против нее, с указанием периода, в течение которого эти голоса были получены;

г) распределение голосов "за" и "против" по субъектам Российской Федерации и муниципальным образованиям (для общественных инициатив соответствующего уровня).

21. [Состав](http://ivo.garant.ru/#/document/72007056/entry/1000) экспертной рабочей группы федерального уровня определяется Правительством Российской Федерации и включает представителей федеральных органов исполнительной власти, депутатов Государственной Думы Федерального Собрания Российской Федерации, членов Совета Федерации Федерального Собрания Российской Федерации, членов Общественной палаты Российской Федерации, представителей бизнес-сообщества и общественных объединений.

22. Состав экспертной рабочей группы регионального уровня определяется высшими органами исполнительной власти субъектов Российской Федерации и включает представителей органов государственной власти Российской Федерации, депутатов представительных (законодательных) органов государственной власти субъектов Российской Федерации, членов общественных палат субъектов Российской Федерации, депутатов представительных органов муниципальных образований, представителей государственных учреждений, бизнес-сообщества и общественных объединений.

23. Состав экспертной рабочей группы муниципального уровня определяется органами местного самоуправления и включает представителей этих органов, депутатов представительных органов муниципальных образований, представителей муниципальных учреждений, бизнес-сообщества и общественных объединений.

24. По результатам рассмотрения общественной инициативы экспертная рабочая группа в срок, не превышающий двух месяцев, готовит экспертное заключение и решение о разработке соответствующего нормативного правового акта и (или) принятии иных мер по реализации инициативы, которые подписываются председателем соответствующей экспертной рабочей группы, о чем уведомляет уполномоченную некоммерческую организацию в электронном виде.

Информация о рассмотрении общественной инициативы и мерах по ее реализации направляется уполномоченной некоммерческой организации для размещения на интернет-ресурсе.

**КОНЦЕПЦИЯ**

**информационной безопасности Российской Федерации**

АННОТАЦИЯ

В Концепции информационной безопасности Российской Федерации (далее — Концепция) на основе анализа современного состояния информационной безопасности определены цели, задачи и ключевые проблемы обеспечения информационной безопасности.

Рассмотрены объекты, угрозы информационной безопасности и возможные их последствия, методы и средства предотвращения, парирования и нейтрализации угроз, а также особенности обеспечения информационной безопасности в различных сферах деятельности государства.

Излагаются основные положения государственной политики обеспечения информационной безопасности в Российской Федерации, организационная структура и принципы построения системы информационной безопасности.

Концепция служит методологической основой разработки комплекса нормативно-правовых и организационно-методических документов, регламентирующих деятельность в области информационной безопасности органов представительной, исполнительной и судебной властей Российской Федерации, субъектов Российской Федерации, органов местного самоуправления (далее — органы государственной власти и управления), предприятий, учреждений и организаций независимо от их организационно-правовой формы и формы собственности (далее — предприятия).

**I. ОБЩИЕ ПОЛОЖЕНИЯ**

***1.1. Назначение, правовая основа Концепции информационной безопасности Российской Федерации***

Концепция информационной безопасности Российской Федерации представляет собой официально принятую систему взглядов на проблему обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере.

Концепция является составной частью Концепции национальной безопасности Российской Федерации и служит методологической основой:

разработки стратегии обеспечения информационной безопасности страны, включающей в себя цели, задачи и комплекс основных мер по ее практической реализации;

формирования и проведения государственной политики Российской Федерации в области обеспечения информационной безопасности;

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

разработки целевых программ защиты информационных ресурсов и средств информатизации.

Положения Концепции должны учитываться при формировании государственной политики информатизации, создания и развития единого информационного пространства России.

Правовую основу Концепции составляют Конституция Российской Федерации, законы Российской Федерации "О безопасности", "О государственной тайне", "Об информации, информатизации и защите информации", другие законодательные акты Российской Федерации, а также международные договоры и соглашения, заключенные или признанные Российской Федерацией, определяющие права и ответственность граждан, общества и государства в информационной сфере.

***1.2. Роль и место информационной безопасности в общей системе национальной безопасности Российской Федерации***

Информационная безопасность играет ключевую роль в обеспечении Жизненно важных интересов Российской Федерации. Это, в первую очередь, обусловлено насущной потребностью, создания развитой и защищенной информационной среды общества. Именно через информационную среду осуществляются угрозы национальной безопасности в различных сферах деятельности государства.

В политической сфере все большее значение приобретают информационные факторы. В традиционном противостоянии политических соперников растут удельный вес и значимость информационно-психологического воздействия.

Экономический потенциал государства все в большей степени определяется объемом информационных ресурсов и уровнем развития информационной инфраструктуры. В то же время растет уязвимость экономических структур от недостоверности, запаздывания и незаконного использования экономической информации.

В военной сфере исход вооружённой борьбы все в большей степени зависит от качества добываемой информации и уровня развития информационных технологий, на которых основываются системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием.

В сфере духовной жизни возникает опасность развития в обществе агрессивной потребительской идеологии, тотальной коммерциализации культуры, распространения идей насилия и нетерпимости, воздействия на психику разрушительных форм мифологизированного сознания. Эти угрозы и защита от них, а также утверждение нравственных ценностей реализуются внутри информационной среды и прежде всего через средства массовой информации и формирования общественного мнения.

Информационная среда, являясь системообразующим фактором во всех сферах национальной безопасности, активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Российской Федерации. В то же время она представляет собой самостоятельную сферу национальной безопасности, в которой необходимо обеспечить защиту информационных ресурсов, систем их формирования, распространения и использования, информационной инфраструктуры, реализацию прав на информацию государства, юридических лиц, граждан.

***1.3. Основные цели и задачи обеспечения информационной безопасности Российской Федерации***

Основные цели обеспечения информационной безопасности определяются на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития, к которым относятся:

сохранение и укрепление российской государственности и политической стабильности в обществе;

сохранение и развитие демократических институтов общества, обеспечение прав и свобод граждан, укрепление законности и правопорядка;

обеспечение достойной роли России в мировом сообществе;

обеспечение территориальной целостности страны;

обеспечение прогрессивного социально-экономического развития России;

сохранение национальных культурных ценностей и традиций.

В соответствии с указанными приоритетами основными целями информационной безопасности являются:

защита национальных интересов России в условиях глобализации информационных процессов, формирования мировых информационных сетей и стремления США и других развитых стран к информационному доминированию;

обеспечение органов государственной власти и управления, предприятий и граждан достоверной, полной и своевременной информацией, необходимой для принятия решений, а также предотвращение нарушений целостности и незаконного использования информационных ресурсов;

реализация прав граждан, организаций и государства на получение, распространение и использование информации.

К основным задачам обеспечения информационной безопасности относятся:

выявление, оценка и прогнозирование источников угроз информационной безопасности;

разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и механизмов ее реализации;

разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности органов государственной власти и управления и предприятий по обеспечению информационной безопасности;

развитие системы обеспечения информационной безопасности, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;

обеспечение активного участия России в процессах создания и использования глобальных информационных сетей и систем.

***1.4. Объекты информационной безопасности Российской Федерации***

К объектам информационной безопасности Российской Федерации относятся:

информационные ресурсы, вне зависимости от форм хранения, содержащие информацию, составляющую государственную тайну и ограниченного доступа, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию и знания;

система формирования, распространения и использования информационных ресурсов, включающая в себя информационные системы различного класса и назначения, библиотеки, архивы, базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический и обслуживающий персонал;

информационная инфраструктура, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации;

система формирования общественного сознания (мировоззрение, политические взгляды, моральные ценности и пр.), базирующаяся на средствах массовой информацией пропаганды;

права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности.

Информационная безопасность всех вышеуказанных объектов создает условия надежного функционирования государственных и общественных институтов, а также формирования общественного сознания, отвечающего прогрессивному развитию страны.

**II. АНАЛИЗ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

***2.1. Основные факторы, влияющие на состояние информационной безопасности Российской Федерации***

Происходящие в настоящее время процессы преобразования в политической жизни и экономике России оказывают непосредственное влияние на состояние ее информационной безопасности. При этом возникают новые факторы, которые необходимо учитывать при оценке реального состояния информационной безопасности и определении ключевых проблем в этой области.

Указанные факторы можно разделить на политические, экономические и организационно-технические.

Политическими факторами являются:

изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира, сведения к минимуму вероятности мировой ядерной и обычной войн;

информационная экспансия США и других развитых стран, осуществляющих глобальный мониторинг мировых политических, экономических, военных, экологических и других процессов, распространяющих информацию в целях получения односторонних преимуществ;

становление новой российской государственности на основе принципов демократии, законности, информационной открытости;

разрушение ранее существовавшей командно-административной системы государственного управления, а также сложившейся системы обеспечения безопасности страны;

нарушение информационных связей вследствие образования независимых государств на территории бывшего СССР;

стремление России к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ на основе максимальной открытости сторон;

низкая общая правовая и информационная культура в российском обществе.

Среди экономических факторов наиболее существенными являются: переход России на рыночные отношения в экономике, появление множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;

критическое состояние отечественных отраслей промышленности, производящих средства информатизации и защиты информации;

расширяющаяся кооперация с зарубежными странами в развитии информационной инфраструктуры России.

Из организационно-технических факторов определяющими являются:

недостаточная нормативно-правовая база в сфере информационных отношений, в том числе в области обеспечения информационной безопасности;

слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг в России;

широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств для хранения, обработки и передачи информации;

рост объемов информации, передаваемой по открытым каналам связи, в том числе по сетям передачи данных и межмашинного обмена;

обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно в кредитно-финансовой сфере.

***2.2. Оценка состояния и ключевые проблемы обеспечения информационной безопасности Российской Федерации***

За последние годы в Российской Федерации реализован комплекс практических мер по совершенствованию информационной безопасности.

Начато формирование нормативно-правового обеспечения информационной безопасности. Приняты законы Российской Федерации "О государственной тайне", "Об информации, информатизации и защите информации", развернуты работы по созданию механизмов их реализации, завершена подготовка ряда законопроектов, регламентирующих деятельность \S субъектов в информационной сфере. Осуществлен ряд практических мероприятий по совершенствованию информационной безопасности в органах государственной власти и управления и на предприятиях. Успешному решению ряда вопросов информационной безопасности способствует создание Государственной системы защиты информации и системы лицензирования деятельности предприятий в области защиты информации.

Вместе с тем, анализ современного состояния информационной безопасности в России показывает, что уровень информационной безопасности в настоящее время не соответствует жизненно важным потребностям личности, общества и государства.

Сегодняшние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями об щества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение.

Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит ко многим негативным последствиям.

Слабое обеспечение органов государственной власти и управления полной, достоверной и своевременной информацией затрудняет принятие обоснованных решений. Неразвитость информационных отношений в сфере предпринимательства тормозит становление цивилизованного рынка. Отсутствие механизма включения информационного ресурса в хозяйственный оборот приводит к серьезным экономическим потерям.

Недостаточная защищенность государственного информационного ресурса приводит к утрате важной политической, экономической и научно-технической информации, в том числе о новых и высокоэффективных технологиях военного и двойного назначения.

Необеспеченность прав граждан на информацию, манипулирование информацией вызывает неадекватную реакцию населения и в ряде случаев ведет к политической нестабильности в обществе.

Потерям важной информации способствуют бессистемность защиты данных и слабая координация мер по защите информации в общегосударственном масштабе, ведомственная разобщенность в обеспечении целостности и конфиденциальности «информации, слабый контроль за экспортом отечественных наукоемких технологий, образцов вооружения и военной техники.

Неблагоприятно обстоят дела с охраной государственной тайны. Серьезно ослаблены меры по обеспечению сохранности государственных секретов, коммерческой и служебной тайны в органах государственной власти и управления и на предприятиях оборонного комплекса.

Гарантированные Конституцией Российской Федерации основные права и свободы, такие как право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, практически не имеют правового, организационного и технического обеспечения. Неудовлетворительно организована защита персональных данных, налоговой, таможенной, имущественной и другой информации.

Продолжается спад производства на государственных предприятиях, в том числе специализирующихся на выпуске защищенной техники, предназначенной для обработки секретной информации. Разрушаются научные и производственные коллективы, наблюдается массовый уход в коммерческие структуры наиболее квалифицированных кадров.

Отставание отечественных информационных технологий вынуждает массового потребителя идти по пути закупок незащищенной импортной техники, в результате чего повышается вероятность несанкционированного доступа к базам и банкам данных, а также возрастает зависимость страны от иностранных производителей компьютерной и телекоммуникационной Техники и информационной продукции.

Такое положение дел в области обеспечения информационной безопасности не позволяет России на равноправной основе включиться в мировую информационную систему и требует безотлагательного решения следующих ключевых проблем:

1. Развития научно-практических основ информационной безопасности, отвечающей современной геополитической ситуации и условиям политического и социально-экономического развития Российской Федерации.

2. Формирования законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, предприятий, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности.

3. Разработки механизмов реализации прав граждан на информацию.

4. Формирования системы информационной безопасности, обеспечивающей реализацию государственной политики в области информационной безопасности.

5. Разработки современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

6. Разработки критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации.

7. Исследований форм и способов цивилизованного воздействия государства на формирование общественного сознания.

8. Комплексного исследования деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

**III. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

***3.1. Источники угроз информационной безопасности Российской федерации***

Источники угроз информационной безопасности в Российской Федерации можно разделить на внешние и внутренние. К внешним источникам относятся:

недружественная политика иностранных государств в области глобального информационного мониторинга, распространения информации и новых информационных технологий;

деятельность иностранных разведывательных и специальных служб;

деятельность иностранных политических и экономических структур, направленная против интересов Российского государства;

преступные действия международных групп, формирований и отдельных лиц;

стихийные бедствия и катастрофы. Внутренними источниками угроз являются:

противозаконная деятельность политических и экономических структур в области формирования, распространения и использования информации;

неправомерные действия государственных структур, приводящие к Нарушению законных прав граждан и организаций в информационной сфере;

нарушения установленных регламентов сбора, обработки и передачи информации;

преднамеренные действия и непреднамеренные ошибки персонала информационных систем;

отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

***3.2. Способы воздействия угроз на объекты информационной безопасности Российской Федерации***

Способы воздействия угроз на объекты информационной безопасности в Российской Федерации подразделяются на информационные, программно-математические, физические, радиоэлектронные, организационно-правовые.

К информационным способам относятся:

нарушения адресности и своевременности информационного обмена, противозаконный сбор и использование информации;

несанкционированный доступ к информационным ресурсам;

манипулирование информацией .(дезинформация, сокрытие или искажение информации);

незаконное копирование данных в информационных системах;

использование средств массовой информации с позиций, противоречащих интересам граждан, организаций и государства;

хищение информации из библиотек, архивов, банков и баз данных;

нарушение технологии обработки информации.

Программно-математические способы включают:

внедрение программ-вирусов;

установку программных и аппаратных закладных устройств; уничтожение или модификацию данных в информационных системах. Физические способы включают:

уничтожение или разрушение средств обработки информации и связи;

уничтожение, разрушение или хищение машинных или других оригиналов носителей информации;

хищение программных или аппаратных ключей и средств криптографической защиты информации;

воздействие на персонал;

поставка "зараженных" компонентов информационных систем.

Радиоэлектронными способами являются:

перехват информации в технических каналах ее утечки;

внедрение электронных устройств перехвата информации в технических средствах й помещениях;

перехват, дешифрование и навязывание ложной информации в сетях передачи данных и линиях связи;

воздействие на парольно-ключевые системы;

радиоэлектронное подавление линий связи и систем управления.

Организационно-правовые способы включают:

закупки несовершенных или устаревших информационных технологий и средств информатизации;

невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере;

неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

***3.3. Возможные последствия воздействия угроз информационной безопасности Российской Федерации***

В результате воздействия угроз информационной безопасности может быть нанесен серьезный ущерб жизненно важным интересам Российской Федерации в политической, экономической, оборонной и других сферах деятельности государства, причинен социально-экономический ущерб обществу и отдельным гражданам.

Вследствие такого воздействия могут быть созданы препятствия на пути равноправного сотрудничества России с развитыми странами и дружественными государствами, затруднено принятие важнейших политических, экономических и других решений, подорван государственный авторитет Российской Федерации на международной арене, создана атмосфера напряженности и политической нестабильности в обществе, нарушен баланс интересов личности, общества и государства, дискредитированы органы государственной власти и управления, спровоцированы социальные, национальные и религиозные конфликты, инициированы забастовки и массовые беспорядки, нарушено функционирование системы государственного управления, а также систем управления войсками, вооружением и военной техникой, объектами повышенной опасности.

Следствием воздействия угроз могут явиться снижение темпов научно-технического развития страны, утрата культурного наследия, проявления бездуховности и безнравственности.

Весьма существенный экономический ущерб в различных областях общественной жизни и в сфере бизнеса может быть причинен в результате нарушений законодательства в информационной сфере и компьютерных преступлений,

Угрозы информационной безопасности могут нанести физический, материальный и моральный ущерб гражданам, вызывать неадекватное социальное и криминальное поведение групп людей или отдельных лиц, оказать влияние на процессы образования и формирования личности.

**IV. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

***4.1. Базовые методы предотвращения, парирования и нейтрализации угроз информационной безопасности Российской Федерации***

В целях предотвращения, парирования и нейтрализации угроз информационной безопасности применяются правовые, программно-технические и организационно-экономические методы.

Правовые методы предусматривают разработку комплекса нормативно-правовых актов и положений, регламентирующих информационные отношения в обществе, руководящих и нормативно-методических документов по обеспечению информационной безопасности.

Программно-технические методы включают предотвращение утечки обрабатываемой информации путем исключения несанкционированного доступа К ней, предотвращение специальных воздействий, вызывающих разрушение; уничтожение, искажение информации или сбои в работе средств информатизации, выявление внедренных программных или аппаратных закладных устройств, исключение перехвата информации техническими средствами, применения криптографических средств защиты информации при передаче по каналам связи.

Организационно-экономические методы предусматривают формирование и обеспечение функционирования систем защиты секретной и конфиденциальной информации, сертификации этих систем по требованиям информационной безопасности, лицензирования деятельности в сфере информационной безопасности, стандартизации способов и средств защиты информации, контроль за действием персонала в защищенных информационных системах.

Важное место среди этих методов занимают мотивация; экономическое стимулирование и психологическая поддержка деятельности персонала, занятого обеспечением информационной безопасности.

***4.2. Особенности обеспечения информационной безопасности в различных сферах, деятельности государства и общегосударственных информационных и телекоммуникационных системах***

Рассмотренные выше объекты, угрозы, методы и средства обеспечения информационной безопасности являются общими для различных сфер деятельности государства.

Вместе с тем, в каждой из этих сфер имеются свои особенности обеспечения информационной безопасности, что в первую очередь связано со спецификой решения поставленных задач, наличием свойственных каждой области информационной безопасности слабых элементов и уязвимых звеньев.

Поэтому в каждой сфере деятельности государства требуется специальная организация работ, использование форм и способов обеспечения информационной безопасности с учетом специфических факторов, влияющих на ее состояние.

***В политической сфере***

Наиболее серьезной опасности в политической сфере подвергаются: общественное сознание и политическая ориентация различных групп населения страны (регионов), непрерывно формируемые под воздействием отечественных и зарубежных средств массовой информации (печать, радио, телевидение);

система принятия политических решений, существенно зависящая от качества и своевременности ее информационного обеспечения;

права политических организаций, партий, объединений и движений на закрепленное в Конституций Российской Федерации свободное выражение своих программ, социально-политических и экономических ориентации через средства массовой информации;

система регулярного информирования населения органами государственной власти и управления о политической и социально-экономической жизни через средства массовой информации, пресс-центры, центры общественных связей и т.п.;

система формирования общественного мнения, включающая специальные институты, центры и службы выявления, изучения и анализа общественного мнения.

Для демократического развития страны наибольшую опасность представляют следующие угрозы:

односторонняя политическая ориентация средств массовой информации под давлением государственных органов, господствующих политических сил, а также под экономическим давлением отдельных групп, в том числе криминальных структур;

пропагандистское и психологическое воздействие на политическую ориентацию населения зарубежных и отечественных средств массовой информации в интересах отдельных политических сил;

отсутствие или несовершенство законодательства, обязывающего органы государственной власти и управления регулярно и полно информировать население о своей деятельности и состоянии дел в сфере своей компетентности;

препятствия со стороны государства осуществлению законных и равных прав различных политических сил, в том числе оппозиционных, на использование средств массовой информации, контролируемых государством;

политизация системы формирования общественного мнения, ведущая к искажению реальных ситуаций (фальсификация или предвзятая интерпретация результатов опросов или референдумов).

Основными мероприятиями обеспечения информационной безопасности в политической сфере являются:

разработка и постоянное совершенствование законодательства, правовых и организационных механизмов, регулирующих взаимоотношения всех субъектов политической жизни в реализации их конституционных прав и обязанностей в использовании средств массовой информации;

создание системы независимого и гласного контроля за деятельностью государственных средств массовой информации, институтов, центров и служб изучения общественного мнения, а также специальных служб по связи с населением;

активизация контрпропагандистской деятельности и дипломатических усилий по предотвращению информационно-пропагандистского вмешательства во внутренние дела страны.

***В сфере экономики***

Среди объектов сферы экономики наиболее подвержены воздействию угроз информационной безопасности: система государственной статистики;

источники, порождающие информацию о коммерческой деятельности хозяйственных субъектов всех форм собственности, о потребительских свойствах товаров и услуг;

системы сбора и обработки финансовой, биржевой, налоговой, таможенной информации, информации о внешнеэкономической деятельности государства и коммерческих структур.

Система государственной статистической отчетности должна обладать достаточной защищенностью от серьезных и массовых искажений. Особое внимание должно уделяться защите первичных источников информации и обобщённых отчетных данных.

В конечном итоге информация в системе государственной статистики должна обладать полнотой, достоверностью, достаточностью, сопоставимостью и регулярностью - свойствами, необходимыми для принятия рациональных решений на уровнях государства, отрасли, предприятия, для проведения общеэкономического анализа и прогнозирования развития народного хозяйства.

Нормальное функционирование хозяйственных объектов нарушается из-за отсутствия нормативно-правовых положений, определяющих ответственность источников информации о коммерческой деятельности и потребительских свойствах товаров Н услуг за недостоверность и сокрытие сведений (о результатах реальной хозяйственной деятельности, об инвестициях и др.). С другой стороны, существенный экономический ущерб может быть нанесен Государственным и предпринимательским структурам вследствие разглашения информации, содержащей коммерческую тайну.

В системах сбора и обработки финансовой, биржевой, налоговой, таможенной информации наибольшую опасность с точки зрения информационной безопасности представляют хищения и преднамеренное искажение информации, возможность которых связана с преднамеренным или случайным Нарушением технологии работы с информацией, несанкционированным доступом к ней, что обусловлено недостаточными мерами защиты информации. Такая же опасность существует в органах, занятых формированием и распространением информации о внешнеэкономической деятельности (центральный аппарат ведомств, торгпредства, таможни и т.п.).

Серьезную опасность для Нормального функционирования сферы экономики в целом представляют все более изощренные компьютерные преступления (подлоги, хищения и т.д.), связанные с проникновением криминальных элементов в компьютерные системы и сети.

Наряду с широким использованием стандартных методов и средств для сферы экономики приоритетными Направлениями обеспечения информационной безопасности являются:

разработка и принятие правовых положений, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ и хищение информации, преднамеренное распространение недостоверной информации, разглашение коммерческой тайны, утечку конфиденциальной информации;

коренная перестройка системы государственной статистической отчетности, направленная на повышение достоверности, полноты, сопоставимости и защищенности информации путем введения строгой юридической ответственности первичных источников информации, организации действенного контроля за их деятельностью и деятельностью служб обработки и анализа статистической информации, ограничения ее коммерциализации, использования специальных организационных и программно-технических средств защиты информации;

создание и совершенствование специальных средств Защиты финансовой и коммерческой информации;

разработка комплекса организационно-технических мероприятий по совершенствованию технологии информационной деятельности и защиты информации в хозяйственных, финансовых, промышленных и других экономических структурах с учетом специфических для сферы экономики требований информационной безопасности;

совершенствование системы профессионального отбора и подготовки персонала систем сбора, обработки, анализа и распространения экономической информации.

***В оборонной сфере***

К объектам информационной безопасности, в оборонной сфере, наиболее уязвимым со стороны всего комплекса угроз, относятся:

информационные ресурсы аппарата Министерства обороны, Генерального штаба, главных штабов видов Вооруженных сил и родов войск, научно-исследовательских учреждений, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, о мобилизационной готовности, тактико-технических характеристиках вооружения и военной техники;

информационные ресурсы предприятий оборонного комплекса, содержащие сведения и данные об их научно-техническом и производственном потенциалах, об объемах поставок и запасах стратегических видов сырья и материалов, об основных направлениях развития вооружения, военной техники, их боевых возможностях и проводимых в интересах обороны фундаментальных и прикладных НИР;

системы связи и управления войсками и оружием, их информационное обеспечение;

политико-моральное состояние войск в части, зависящей от информационно-пропагандистского воздействия;

информационная инфраструктура, в том числе центры обработки и анализа информации Генерального штаба и информационные подразделения штабов видов Вооруженных Сил, штабов объединений и соединений видов Вооруженных Сил и родов войск, пункты управления, узлы и линии радио-, радиорелейной, тропосферной и спутниковой связи, а также линии проводной связи, развертываемые и арендуемые Министерством обороны и другими силовыми структурами.

Из внешних источников угроз в наибольшей степени способны воздействовать на информационную безопасность объектов оборонной сферы следующие:

все виды разведывательной деятельности зарубежных государств;

информационно-технические воздействия (методы радиоэлектронной борьбы, проникновение в компьютерные сети и т.п.) со стороны вероятных противников;

психологические операции вероятных противников, осуществляемые специальными методами и через деятельность средств массовой информации;

деятельность иностранных политических и экономических структур, направленная против интересов Российской Федерации в оборонной сфере.

Из внутренних источников угроз наибольшую опасность представляют:

нарушение- установленных регламентов сбора, обработки и передачи информации в штабах и учреждениях Министерства обороны, в организациях и на предприятиях оборонного комплекса;

преднамеренные действия и непреднамеренные ошибки персонала информационных систем специального назначения;

отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах специального назначения;

информационно-пропагандистская деятельность организаций и отдельных лиц, направленная против интересов государства, подрывающая престиж вооруженных сил и их боеготовность.

Эти источники угроз представляют особую опасность в условиях обострения военно-политической обстановки.

Главными направлениями совершенствования информационной безопасности в оборонной сфере являются:

концептуальное, включающее структуризацию целей обеспечения информационной безопасности в оборонной сфере, вытекающих из них практических задач, корректное определение информационных угроз и их источников;

техническое, характеризуемое постоянным совершенствованием средств защиты информационных ресурсов от методов и средств несанкционированного доступа к ним, развитием защищенных, засекреченных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

организационное, связанное с необходимостью формирования оптимальной структуры и состава функциональных органов системы информационной безопасности в оборонной сфере и координации их аффективного взаимодействия, совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника.

Кроме того, одним из главных направлений совершенствования информационной безопасности в оборонной сфере является повышение эффективности защиты технологий производства и тактико-технических характеристик вооружения и военной техники. 9

***В условиях чрезвычайных ситуаций***

Наиболее уязвимыми объектами для угроз информационной безопасности в условиях чрезвычайных ситуаций (ЧС) являются система принятия решений по оперативным действиям (реакциям) на их развитие и ход ликвидации последствий, а также система сбора и обработки информации о возможном возникновении ЧС.

Особое значение для нормального функционирования этих объектов имеет разрушение информационной инфраструктуры (центров сбора и анализа информации, технических средств обработки и передачи информации, систем телекоммуникации и каналов связи) вследствие аварий, катастроф и стихийных бедствий. Эти события, а также задержка, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп людей могут привести к тяжелым последствиям.

Особенностью информационного воздействия в условиях ЧС является приведение в движение больших масс людей, испытывающих психический стресс, быстрое распространение панических слухов, ложной или недостоверной информации. Нередко в условиях ЧС имеет место сокрытие информации, приводящее к сложностям при ликвидации ее последствий.

К специфическим для данной сферы направлениям обеспечения информационной безопасности относятся:

разработка эффективной системы мониторинга признаков — предвестников ЧС;

повышение надежности средств обработки и передачи информации, обеспечивающих деятельность центров принятия решений по ЧС;

анализ поведения больших масс людей под воздействием ложной или недостоверной информации и выработка мер по управлению ими в условиях ЧС;

разработка специальных мер повышения информированности населения в условиях ЧС.

***В общегосударственных информационных и телекоммуникационных системах***

Основными объектами информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются:

информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию, представленные в виде документированных информационных массивов и баз данных;

средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации (звукозаписи, звукоусиления, звукосопровождения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), используемые для обработки информации ограниченного доступа, их информативные физические поля;

технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается (циркулирует) информация, содержащая сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для секретных переговоров.

Основными источниками угроз в сфере информационной безопасности являются деятельность иностранных разведывательных и специальных служб, преступных групп и формирований, противозаконная деятельность отдельных лиц, нарушение установленных регламентов сбора, обработки и передачи информации, преднамеренные действия и непреднамеренные ошибки персонала информационных систем, отказы технических средств и сбои программного обеспечения в информационных и телекомуникационных системах.

Основными направлениями обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах являются:

предотвращение перехвата с помощью технических средств информации, передаваемой по каналам связи;

исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразовании;

предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

предотвращение перехвата техническими средствами речевой информации из помещений и объектов.

Предотвращение перехвата с помощью технических средств информации, передаваемой по каналам связи, достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий.

Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации И другими организационными и техническими мерами.

Предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигается применением специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), организацией системы контроля безопасного программного обеспечения.

Выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) достигается проведением специальных проверок.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

лицензирование деятельности предприятий в области защиты информации;

аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

разработка и использование средств защиты информации и методов контроля за ее эффективностью;

применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случаях ее утечки, разрушения или уничтожения.

***В области науки и техники***

Наиболее уязвимыми объектами информационной безопасности в области науки и техники являются:

результаты фундаментальных, поисковых и прикладных научных исследований, содержащие сведения, данные и знания, потенциально важные для научно-технического, технологического и социально-экономического развития страны, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

незапатентованные технологии, ноу-хау, промышленные образцы, модели и экспериментальное оборудование, для которых еще не определен статус конфиденциальности и Которые поэтому не подпадают под действующее законодательство и могут быть проданы или переданы за рубеж;

объекты интеллектуальной собственности (открытия, патенты, изобретения, промышленные образцы, программные продукты и пр.), которые могут быть похищены и незаконно распространены или использованы, несмотря на их правовую защиту.

Специфика угроз перечисленным объектам информационной безопасности состоит в их многообразии, сложности идентификации, поскольку, как правило, они носят уникальный или индивидуальный характер» При классификации угроз в этой области необходимо уделять особое внимание изучению возможности промышленного шпионажа специальных служб и криминальных структур.

Вследствие этой специфики объекты информационной безопасности в области науки, техники и технологии трудно защитимы. Должна быть организована система оценки возможных последствий воздействия угроз на указанные объекты, включающая общественные научные советы и институт независимых экспертиз, вырабатывающие рекомендации для каждого конкретного случая распространения или использования научной, технической и технологической продукции с целью предотвращения незаконного присвоения или Использования научного и интеллектуального потенциала.

Реальный Путь противодействия угрозам со стороны государства заключается в постоянном совершенствовании законодательства в этой области и механизмов его реализации. Многие мероприятия по предотвращению или нейтрализации угроз в этой области, особенно в части, касающейся научных кадров, лежат в сфере социальной и экономической политики государства.

***В сфере духовной жизни и информационной безопасности личности***

Объектами информационной безопасности в духовной сфере являются мировоззрение людей, их жизненные ценности и идеалы, социальные и личностные ориентации, их культурные и эстетические позиции. Оценка последствий тех или иных информационных воздействий в этой сфере весьма затруднительна и должна производиться с учетом конкретно складывающейся обстановки.

Сфера духовной жизни весьма чувствительна к информационно-пропагандистскому воздействию, идеологическому давлению, культурной экспансии, которые осуществляются, главным образом, через средства массовой информации и могут рассматриваться как информационные угрозы духовному здоровью населения страны. Средства массовой информации играют определяющую роль в формировании духовной жизни. В этом состоит их особая ответственность перед обществом.

Сами информационные воздействия осуществляются в гибких, постоянно изменяющихся формах, что обусловливает сложность определения их влияния на различные составляющие духовной сферы. Это особенно характерно для современного периода развития России, когда по существу не сформулированы национальные приоритеты и идеология перестраивающихся общества и государства.

Предотвращение и нейтрализация угроз информационной безопасности в сфере духовной жизни требуют, прежде всего, открытого провозглашения государственной, официальной идеологии, приемлемой для большинства населения и учитывающей культурные и исторические традиции многонациональной страны. Лишь на основе такой идеологии могут быть выработаны четкие критерии оценки угроз информационной безопасности, основные приоритеты и государственная политика в этой сфере.

Главным представляется разработка и осуществление цивилизованных, демократических форм и методов воздействия на средства массовой информации в целях формирования и распространения духовных ценностей, отвечающих национальным интересам страны, воспитания гражданского и патриотического долга и защиты от враждебной или недружественной пропаганды.

Необходимо также разработать специальные правовые и организационные мероприятия, препятствующие коммерциализации культуры и обеспечивающие сохранение и развитие информационных ресурсов, составляющих большую культурно-историческую ценность.

Основным носителем духовных ценностей является личность, постоянно испытывающая информационные воздействия, направленные на формирование ее отношения к действительности, идеалов и устремлений, мотиваций и уровня притязаний. Эти воздействия могут создавать эмоциональный дискомфорт, вызывать стрессы и нарушать физическую, социальную или духовную целостность личности.

Обеспечение информационной безопасности личности означает ее право на получение объективной информации и предполагает, что полученная человеком из разных источников информация не препятствует свободному формированию и развитию его личности. В качестве воздействия на личность может выступать:

целенаправленное информационное давление с целью изменения мировоззрения, политических взглядов и морально-психологического состояния людей;

распространение недостоверной, искаженной, неполной информации; использование неадекватного восприятия людьми достоверной информации.

Особую роль в воздействии на сознание и поведение отдельной личности играют средства массовой информации, которые в силу своей общедоступности и распространенности оказывают непосредственное влияние на мировоззренческие установки, субъективные ценности и предпочтения, регуляцию поступков и взаимодействие с другими людьми.

При организации противодействия угрозам информационной безопасности личности необходимо учитывать индивидуальные и личностные особенности людей, сформированные предыдущим опытом, мотивами и интересами, интеллектуальным уровнем, социально-демографическими характеристиками, социальным статусом, стереотипами и другими факторами.

Выбор адекватных способов воздействия (убеждения, внушения, разъяснения), адекватных средств (аудио, визуальных, электронных, печатных) зависят от полноты учета всех характеристик личности и ситуации. Одним из важнейших способов противодействия является упреждающее информационное воздействие.

Устойчивость к воздействиям извне определяется личностными качествами человека, которые во многом определяются постоянными информационными воздействиями, главным образом со стороны средств массовой информации. Они несут основную ответственность за формирование личностных и гражданских качеств, способных противостоять информационным угрозам. Особенно это важно в настоящее время, когда в обществе проявляются низкий уровень правосознания, непонимание людьми ценности информации.

Информационные угрозы, вызывающие сознательные или непреднамеренные нарушения информационной безопасности лиц, работающих в информационных системах и средствах массовой информации, должны парироваться посредством разъяснения их прав, регламентации обязанностей и разделения ответственности, обучения и тренинга персонала, а в особо важных случаях — путем отбора специалистов по психологическим критериям.

**V. ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

***5.1. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации***

Государственная политика обеспечения информационной безопасности в Российской Федерации (далее — Государственная политика) формирует направления деятельности органов государственной власти и управления в области обеспечения информационной безопасности, включая гарантии прав всех субъектов на информацию, закрепление обязанностей и ответственности государства и его органов за информационную безопасность страны, и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учетом ограничений, предусмотренных действующим законодательством.

Государственная политика исходит из принципа безусловного правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Она основывается на обязательном обеспечении прав граждан и организаций на свободное создание, поиск, получение и распространение информации любым законным способом, В этих целях государство совершенствует существующее и разрабатывает новое законодательство и нормативно-правовую базу информационных отношений в обществе, а также осуществляет контроль за безусловным их исполнением.

Государство исходит из того, что информационные ресурсы являются объектом собственности, способствует введению их в хозяйственный оборот при соблюдении законных интересов собственников, владельцев и распорядителей информационных ресурсов.

Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и технических средств, способных обеспечить создание национальных телекоммуникационных сетей и включение России в глобальные информационные сети и системы мониторинга.

Исходя из принципа разделения ответственности между органами федеральной, региональной власти и местного самоуправления, государственная политика предусматривает согласованность организационных и технических решений, принимаемых этими органами для обеспечения информационной безопасности в рамках единого информационного пространства России.

Государственная политика не допускает монополизма министерств, ведомств и организаций в области обеспечения информационной безопасности.

Государственная политика обеспечения информационной безопасности исходит из следующих основных положений:

ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

ответственность за сохранность информации, ее засекречивание и рассекречивание персонифицируется;

доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

юридические и физические лица, собирающие, накапливающие и обрабатывающее персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через средства массовой информации;

государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

государство формирует Федеральную программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности России;

государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем.

На основе изложенных принципов и положений определяются общие направления формирования и реализации политики информационной безопасности в политической, военной, экономической и других сферах деятельности государства.

Государственная политика в качестве механизма Согласования интересов субъектов информационных отношений и нахождения компромиссных решений предусматривает формирование и организацию эффективной работы различных советов, комитетов и комиссий с широким представительством специалистов, и всех заинтересованных структур.

Механизмы реализации Государственной политики должны быть гибкими и своевременно отражать изменения, происходящие в политической и экономической жизни страны.

***5.2. Основные положения государственной политики обеспечения информационной безопасности субъектов Российской Федерации***

Конституционные основы федеративного государственного устройства страны нуждаются в развитии и распространении на все сферы жизнедеятельности личности, общества и государства, включая сферу обеспечения информационной безопасности.

Информационная безопасность должна быть предметом ответственности органов государственной власти и управления всех уровней с учетом закрепленного в Конституции Российской Федерации разграничения предметов ведения и полномочии между ними.

Разработка региональных вопросов обеспечения информационной безопасности имеет ряд особенностей, объективно связанных с федеративным устройством страны.

Информационная собственность субъектов Российской Федерации является разновидностью государственной собственности субъектов Российской Федерации.

Она включает в себя:

информационную собственность органов власти и управления субъектов Российской Федерации;

информационную собственность предприятий и учреждений, созданных или приобретенных за счет средств субъектов Российской Федерации;

культурные ценности народов, населяющих территорию субъектов Российской Федерации.

Обязанностью органов власти и управления субъектов Российской Федерации является защита права информационной собственности, находящейся на территории субъектов1 Российской Федерации объектов федеральной информационной собственности, информационной собственности органов местного, самоуправления, других юридических и физических лиц.

Субъекты Российской Федерации обладают всей полнотой информационных прав, действующих в Российской Федерации. Эти права от имени субъектов Российской Федерации осуществляют их органы государственной власти и управления.

Субъектам Российской Федерации гарантируется:

равное право доступа на российский рынок информации и средств обеспечения информационной безопасности, находящихся в любой форме собственности;

право использования для решения региональных государственных задач федеральных информационных банков данных с соблюдением установленных правил обеспечения информационной безопасности;

право проведения самостоятельной внутренней и внешнеэкономической деятельности в сфере информационной безопасности в рамках, определенных федеральными законами;

право осуществлять защиту своих информационных прав и права информационной собственности как самостоятельно, так и путем обращения в федеральные и международные правозащитные органы.

Более подробная проработка основных направлений региональной политики обеспечения информационной безопасности должна быть осуществлена субъектами Российской федерации с учетом особенностей их территорий, состояния и перспектив развития хозяйственной сферы.

***5.3. Правовое обеспечение информационной безопасности Российской Федерации***

Правовое обеспечение рассматривается как приоритетное направление формирования механизмов реализации политики обеспечения информационной безопасности в Российской Федерации.

Правовое обеспечение включает в себя:

нормотворческую деятельность по созданию законодательства, регулирующего отношения в обществе, связанные с обеспечением информационной безопасности;

исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации и защиты информации органами государственной власти и управления, организациями (юридическими лицами), гражданами.

Нормотворческая деятельность в области обеспечения информационной безопасности предусматривает:

оценку состояния действующего законодательства и разработку программы его совершенствования;

создание организационно-правовых механизмов обеспечения информационной безопасности;

формирование правового статуса всех субъектов в системе информационной безопасности, пользователей информационных и телекоммуникационных систем и определение их ответственности за обеспечение информационной безопасности;

разработку организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учетом всех видов (категорий) информации;

разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействий угроз, восстановления нарушенного права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность предусматривает разработку процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией и\* нарушившим регламент информационных взаимодействий, а также правонарушения с использованием незащищенных средств информатизации, разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности.

Вся деятельность по правовому обеспечению информационной безопасности должна строиться на основе трех фундаментальных положений права — соблюдение законности, обеспечение баланса интересов отдельных субъектов и государства, неотвратимость наказания.

Соблюдение законности предполагает Наличие законов и иных нормативных установлений, их применение и исполнение субъектами права в области информационной безопасности.

Обеспечение баланса интересов граждан, других субъектов информационных отношений и государства предусматривает приоритет государственных интересов как общих интересов всех субъектов. Ориентация на свободы, права и интересы граждан не принижает роль государства в обеспечении национальной безопасности в целом и в области информационной безопасности в частности.

Неотвратимость наказания предусматривает соответствующую степень ответственности в области обеспечения информационной безопасности, которая реализуется с учетом повышенной социальной опасности угроз информационной среде общества.

Реализация механизмов правового обеспечения информационной безопасности должна опираться на информатизацию правовой сферы в целом.

***5.4. Первоочередные мероприятия по реализации государственной политики информационной безопасности Российской Федерации***

Первоочередные мероприятия по реализации государственной политики информационной безопасности Российской Федерации должны включать:

разработку форм, методов и средств реализации государственной политики, подготовку решений органов исполнительной власти и документов, закрепляющих ее основные положения;

создание нормативно-правовой базы реализации государственной политики в области информационной безопасности, в том числе определение последовательности и порядка разработки законодательных и нормативно-правовых актов, а также механизмов практической реализации принятого законодательства;

анализ технико-экономических параметров отечественных и зарубежных программно-технических средств обеспечения информационной безопасности и выбор перспективных направлений развития отечественной техники;

формирование Государственной научно-технической программы совершенствования и развития методов и средств обеспечения информационной безопасности, предусматривающей их использование в национальных информационных и телекоммуникационных сетях и системах с учетом перспективы вхождения России в глобальные информационные сети и системы;

создание системы сертификации на соответствие требованиям информационной безопасности отечественных и закупаемых импортных средств информатизации, используемых в государственных органах власти и управления;

совершенствование организационной структуры системы информационной безопасности Российской. Федерации, предусматривающее создание единого центра координации и регулирования деятельности всех органов, входящих в систему;

разработка системы экономических и статистических показателей, характеризующих эффективность функционирования системы обеспечения информационной безопасности;

определение реальных потребностей системы информационной безопасности в специалистах, организация системы отбора, подготовки и переподготовки кадров.

**VI. ОРГАНИЗАЦИОННАЯ СТРУКТУРА И ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

***6.1. Организационная структура системы информационной ■ безопасности Российской Федерации***

Анализ состояния информационной безопасности в стране диктует необходимость реформирования существующей организации обеспечения информационной безопасности с целью создания целостной, системы обеспечения информационной безопасности Российской Федерации (далее — Система).

Система является составной частью общей системы национальной безопасности страны, представляет собой совокупность органов государственной власти и управления и предприятий, согласованно осуществляющих, деятельность по обеспечению' информационной безопасности на основе единых правовых норм.

Организационную структуру Системы составляют:

органы государственной власти и управления Российской Федерации и субъектов Российской Федерации, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;

государственные и межведомственные комиссии и советы, специализирующиеся на проблемах информационной безопасности;

структурные и межотраслевые подразделения по защите информации органов государственной власти и управления, а также структурные подразделения предприятий, проводящие работы с использованием сведений, отнесенных к государственной тайне, или специализирующиеся на проведении работ в области защиты информации;

научно-исследовательские, проектные и конструкторские организации, выполняющие работы по обеспечению информационной безопасности;

учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения информационной безопасности.

Особое место в системе информационной безопасности занимают государственные и общественные организации, осуществляющие законный контроль за деятельностью государственных и негосударственных средств массовой информации.

***6.2. Основные функции системы информационной безопасности Российской Федерации***

Система информационной безопасности осуществляет свою деятельность на основе государственной политики обеспечения национальной безопасности Российской Федерации.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

разработка и реализация стратегии обеспечения информационной безопасности;

реализация прав граждан и организаций на получение, распространение и использование информации;

оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, парирования и нейтрализации этих угроз;

координация и контроль деятельности субъектов системы информационной безопасности;

организация разработки федеральных и ведомственных программ обеспечения информационной безопасности и координация работ по их реализации;

проведение единой технической политики в области обеспечения информационной безопасности;

организация фундаментальных, поисковых и прикладных научных исследований в области информационной безопасности;

обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в области защиты информации и сертификации средств защиты информации;

осуществление международного сотрудничества в сфере информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Система должна обеспечивать гибкое управление процессами информационной безопасности на государственном, региональном, отраслевом, производственном и пользовательском уровнях.

Масштабность, сложность и разнообразие перечисленных функций требуют создания иерархической организационной структуры, обеспечивающей координацию деятельности всех составляющих системы информационной безопасности.

Построение Системы осуществляется на основе разграничения предметов ведения и полномочий федеральных и региональных органов государственной власти, с учетом согласованности деятельности территориальных органов федеральной исполнительной власти и органов власти субъектов Российской Федерации.

**VII. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Международное сотрудничество в области информационной безопасности (далее — сотрудничество) есть неотъемлемая составляющая политического, военного, экономического, культурного й других видов взаимодействия стран — участников мирового сообщества.

Сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Российскую Федерацию.

Основными направлениями сотрудничества, отвечающими интересам Российской Федерации, являются:

предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских сетях и в каналах информационного обеспечения мировой торговли, к конфиденциальной информации в международных политических, экономических и военных союзах, блоках и организациях, к информации в международных правоохранительных организациях, ведущих борьбу с международной организованной преступностью, международным терроризмом, распространением наркотиков и незаконной торговлей оружием и расщепляющимися материалами;

обеспечение информационной безопасности трансграничного информационного обмена и его информационного регламента, а также сохранности и неискаженности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности государств — участников международного сотрудничества по предотвращению компьютерных преступлений.

Особое внимание в ходе сотрудничества должно быть уделено проблемам взаимодействия со странами СНГ с учетом перспектив создания единого информационного пространства на территории бывшего СССР, в пределах которого используются практически единые телекоммуникационные системы и линии связи.

Для реализации указанных направлений сотрудничества необходимо:

активное участие России во всех международных организациях, действующих в области информационной безопасности;

обмен опытом в области обеспечения информационной безопасности, в том числе через международные и отечественные печатные издания;

расширение участия российских специалистов в международных конференциях, семинарах, выставках.

Для разработки методологических и научно-технических проблем обеспечения международной информационной безопасности целесообразно создание под эгидой ООН Международного научно-исследовательского института.

***ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ***

***Документированная информация*** - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

***Защита информации*** - организационные, правовые, технические и технологические меры по предотвращению угроз информационной безопасности и устранению их последствий.

***Информационная безопасность*** - состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства.

***Информационная среда*** - совокупность информационных ресурсов, общества система формирования, распространения и использования информации, информационной инфраструктуры.

***Информационная инфраструктура*** - совокупность центров обработки и анализа информации, каналов информационного обмена и телекоммуникации, линий связи, систем и средств защиты информации.

***Информация*** - сведения о лицах, предметах, событиях, явлениях и процессах, независимо от формы их представления.

***Информационные ресурсы*** - данные и документированная информация о жизнедеятельности общества, организованная, в базы и банки данных, а также другие формы организации информации.

***Угрозы информационной безопасности*** - фактор или совокупность факторов, создающих опасность функционированию и развитию информационной среды общества.

***Информация с ограниченным доступом*** - информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования.

***Несанкционированный доступ к информации*** - доступ к информации, нарушающий установленные правила получения информации.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ

ОБЩЕГО ОБРАЗОВАНИЯ

ПИСЬМО

от 14 мая 2018 г. N 08-1184

О НАПРАВЛЕНИИ ИНФОРМАЦИИ

Департамент государственной политики в сфере общего образования Минобрнауки России направляет для сведения разработанные Временной комиссией Совета Федерации по развитию информационного общества методические [рекомендации](http://legalacts.ru/doc/pismo-minobrnauki-rossii-ot-14052018-n-08-1184-o-napravlenii/#100008) о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет".

Директор Департамента

А.Е.ПЕТРОВ

Приложение

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

О РАЗМЕЩЕНИИ НА ИНФОРМАЦИОННЫХ СТЕНДАХ, ОФИЦИАЛЬНЫХ

ИНТЕРНЕТ-САЙТАХ И ДРУГИХ ИНФОРМАЦИОННЫХ РЕСУРСАХ

ОБЩЕОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ И ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ

УПРАВЛЕНИЕ В СФЕРЕ ОБРАЗОВАНИЯ, ИНФОРМАЦИИ О БЕЗОПАСНОМ

ПОВЕДЕНИИ И ИСПОЛЬЗОВАНИИ СЕТИ "ИНТЕРНЕТ"

Экспертами и членами Временной комиссии Совета Федерации по развитию информационного общества в рамках выполнения рекомендаций парламентских слушаний "Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве", которые прошли в Совете Федерации 17 апреля 2017 г., были разработаны методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет" (далее - методические рекомендации).

Методические рекомендации направлены на качественное повышение уровня информационной деятельности общеобразовательных организаций и органов, осуществляющих управление в сфере образования, в части информирования учащихся, их родителей (законных представителей) и педагогических работников об основных аспектах информационной безопасности.

Методические рекомендации позволят общеобразовательным организациям и органам, осуществляющим управление в сфере образования, актуализировать уже используемые и размещенные информационные материалы, так и подготовить их в случае их отсутствия с учетом лучших практик и рекомендаций.

В рамках методических рекомендаций рассматриваются следующие инструменты:

1. информационные стенды;

2. официальные интернет-ресурсы;

3. средства массовой информации (школьные газеты, педагогические издания и другие).

Информационные стенды

На информационных стендах в общеобразовательных организациях, расположенных в фойе учреждений и в кабинетах, оснащенных персональными устройствами для выхода в сеть "Интернет", рекомендуется разместить информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.

В [приложении N 1](http://legalacts.ru/doc/pismo-minobrnauki-rossii-ot-14052018-n-08-1184-o-napravlenii/#100055) к методическим рекомендациям представлен образец памятки для размещения на информационных стендах.

Средства массовой информации

В средствах массовой информации, ориентированных на обучающихся, рекомендуется в течение учебного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности, а также различные памятки общего характера.

В средствах массовой информации, ориентированных на педагогическую общественность, рекомендуется в течение календарного года регулярно публиковать информационные материалы, посвященные отдельным аспектам информационной безопасности как несовершеннолетних, так и общеобразовательных организаций, а также различные памятки, обзоры нормативно-правового регулирования данной сферы и информацию о актуальных мероприятиях и событиях в данной сфере.

В ходе проведения Единого урока по безопасности в сети "Интернет" рекомендуется обеспечить выпуск тематического выпуска средства массовой информации либо серии публикаций, среди которых рассмотреть организованные мероприятия для обучающихся, их родителей (законных представителей) и педагогической общественности.

Официальные Интернет-ресурсы

Общеобразовательным организациям рекомендуется на своих официальных Интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела "Информационная безопасность", в рамках которого предусмотреть размещение следующей информации:

|  |  |  |  |
| --- | --- | --- | --- |
| N | Раздел/подраздел | Формат представления материалов | Содержание материалов |
| 1. | Локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся | Копии документов в формате \*PDF | Размещаются копии документов, т.е. сканированный вариант документа, соответствующий требованиям к параметрам сканирования. Размещаются документы, регламентирующие организацию и работу с персональными данными, планы мероприятий по обеспечению информационной безопасности обучающихся и другие. |
| 2. | Нормативное регулирование | Копии документов в формате \*PDF | Публикуются актуальные сведения о федеральных и региональных законах, письмах органов власти и другие нормативно-правовые документы, регламентирующие обеспечение информационной безопасности несовершеннолетних. Допускается вместо копий размещать гиперссылки на соответствующие документы на сайтах органов государственной власти. |
| 3. | Педагогическим работникам | Текст на странице сайта  Копии документов в формате \*PDF | Размещаются методические рекомендации и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников. |
| 4. | Обучающимся | Текст на странице сайта | Размещается информационная памятка [(приложение N 2)](http://legalacts.ru/doc/pismo-minobrnauki-rossii-ot-14052018-n-08-1184-o-napravlenii/#100075) и указывается информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности обучающихся. |
| 5. | Родителям (законным представителям) обучающихся | Текст на странице сайта | Размещается информационная памятка [(приложение N 3)](http://legalacts.ru/doc/pismo-minobrnauki-rossii-ot-14052018-n-08-1184-o-napravlenii/#100194). |
| 6. | Детские безопасные сайты | Текст на странице сайта | Размещается информация о рекомендуемых к использованию в учебном процессе безопасных сайтах, баннеры безопасных детских сайтов. |

Органам, осуществляющим управление в сфере образования, рекомендуется на своих официальных Интернет-ресурсах обеспечить функционирование самостоятельного и специализированного раздела "Информационная безопасность", в рамках которого предусмотреть размещение следующей информации:

**Информация о мероприятиях, проектах и программах,**

**направленных на повышение информационной грамотности**

**педагогических работников**

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ПО ОБУЧЕНИЮ УЧАЩИХСЯ ПРАВИЛАМ БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ, ПРОФИЛАКТИКЕ ИНТЕРНЕТ-ЗАВИСИМОСТИ

Методические рекомендации разработаны с целью обеспечения реализации образовательными организациями системы мероприятий, направленных на обучение учащихся правилам безопасного поведения в интернет-пространстве, профилактику интернет-зависимости, националистических проявлений в молодежной среде и устранение риска вовлечения подростков в противоправную деятельность. Рекомендации разработаны на основании письма Министерства образования и науки Мурманской области от 12.12.2014 №17-02/9115-ИК «О методическом обеспечении деятельности по противодействию экстремизму среди обучающихся и профилактике интернет-зависимости».

Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 No 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

В Интернете, как и в реальной жизни, учащихся подстерегают опасности: доступность нежелательного контента в социальных сетях, обман и вымогательство денег, платные СМС на короткие номера, пропаганда насилия и экстремизма, игромания и интернет-зависимость, склонение к суициду и т. п.

Интернет-зависимость — это навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. В частности, некоторые учащиеся настолько увлекаются виртуальным пространством, что начинают предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Видами интернет-зависимости являются навязчивый веб-серфинг, пристрастие к виртуальному общению и виртуальным знакомствам (большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети), игровая зависимость — навязчивое увлечение компьютерными играми по сети.

Задача педагогов в связи с имеющимися рисками состоит в том, чтобы указать на эти риски, предостеречь от необдуманных поступков, сформировать у учащихся навыки критического отношения к получаемой в Интернете информации, воспитать культуру безопасного использования Интернет. Также следует обратить внимание на гигиенические требования, которые необходимо соблюдать при работе с компьютером:

* школьникам среднего и старшего возраста можно проводить перед монитором до двух часов в день, устраивая 10-15-минутные перерывы каждые полчаса;
* ребенок младшего возраста может находиться за компьютером не более 15 минут в день, в условиях классно-урочной деятельности – не более одного урока, а при наличии противопоказаний офтальмолога – только 10 минут, не более 3 раз в неделю;
* лучше работать за компьютером в первой половине дня;
* комната должна быть хорошо освещена;
* при работе за компьютером следить за осанкой, мебель должна соответствовать росту;
* расстояние от глаз до монитора – 60 см;
* периодически делать зарядку для глаз.

В соответствии с федеральными государственными образовательными стандартами общего образования в структуру основной образовательной программы основного общего образования включена программа воспитания и социализации учащихся, которая содержит такое направление, как формирование культуры здорового и безопасного образа жизни. В рамках этой программы может осуществляться информационно-просветительская работа среди школьников, пропагандирующая важность владения навыками безопасной работы в сети Интернет.

В образовательных организациях необходимо проводить занятия для учащихся по основам информационной безопасности («основы медиа- безопасности»); знакомить родителей с современными программно- техническими средствами (сетевыми фильтрами, программами «родительский контроль»), ограничивающими доступ детей и подростков к ресурсам сети Интернет, несовместимыми с задачами воспитания; проводить специальные мероприятия по вопросам информационной безопасности несовершеннолетних.

В качестве возможного варианта предоставления учащимся соответствующих знаний может быть использована учебная программа

«Интернет: возможности, компетенции, безопасность», разработанной специалистами факультета психологии МГУ им. М.В. Ломоносова,Федерального института развития образования и Фонда Развития Интернет, рекомендованная Министерством образования и науки РФ ([http://detionline.com](http://detionline.com/)– главная страница, <http://detionline.com/internet-project/about><http://detionline.com/assets/files/research/BookTheorye.pdf>теория, <http://detionline.com/assets/files/research/Book_Praktikum.pdf>— практика)

Содержание программы направлено на обучение учащихся полезному и безопасному использованию сети Интернет и социальных сетей, обучению критической оценке онлайн контента и навыкам сетевой коммуникации. Авторами программы разработано методическое пособие для преподавателей и практикумы для проведения уроков, а также запущен интернет-ресурс

«Разбираем Интернет» ([www.razbiraeminternet.ru](http://www.razbiraeminternet.ru/)). На этом сайте в игровой форме представлены мультимедийные средства обучения для детей и подростков, надо рекомендовать обучающимся посещать этот сайт.

Содержательная часть и объем учебного курса может определяться индивидуально, в зависимости от потребностей конкретной общеобразовательной организации и учащихся. Обучение навыкам безопасного и эффективного использования интернет-ресурсов возможно в рамках учебного курса «Основы безопасности жизнедеятельности» и в рамках программ факультативов, кружков, элективных курсов, а также индивидуальных учебных планов, реализуемых образовательными организациями. Материалы бесплатны и доступны для скачивания [www.razbiraeminternet.ru/teacher](http://www.razbiraeminternet.ru/teacher).

Академией повышения квалификации и профессиональной переподготовки работников образования (г.Москва) разработан учебно- методический комплект «Здоровье и безопасность детей в мире компьютерных технологий и Интернет». УМК разработан с учетом потребностей образовательных организаций в области безопасной работы в Интернет и ориентирован на руководителей, методистов, педагогов, заинтересованных в повышении своей компетентности в области безопасного применения ИКТ. Методическое приложение к программе можно использовать при организации просветительской работы с родителями и учащимися. <https://edu.tatar.ru/upload/images/files/children_health_and_care_in_it.pdf>

Рекомендации по безопасному использованию Интернета для несовершеннолетних и их родителей даны и на сайте Майкрософт.

<http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx>, [http://www.microsoft.com/ru-](http://www.microsoft.com/ru-ru/security/default.aspx) [ru/security/default.aspx.](http://www.microsoft.com/ru-ru/security/default.aspx)

Вышеуказанные сетевые ресурсы могут быть использованы для проведения педсоветов в образовательных организациях по вопросам безопасности детей в сети Интернет.

Рекомендуется провести анкетирование обучающихся и родителей по вопросам безопасного использования сети Интернет. Вопросы для анкетирования учащихся и родителей представлены на сайте «Детионлайн»

<http://detionline.com/internet-project/competence-research>.

В письме Министерства образования и науки РФ от 25.12.13 № НТ- 1338/08 об учебной программе «Интернет: возможности, компетенции, безопасность» предлагаются модели уроков по вышеуказанной теме, даются рекомендации для учёта возрастных особенностей учащихся.

<http://www.dagminobr.ru/documenty/informacionnie_pisma/pismo_3431018_ot_29_yanvarya_2014_g/print>.

При работе с младшими школьниками целесообразно использовать игровые методы, в том числе и Интернет — игру «Прогулка через Дикий Интернет Лес» (<http://www.wildwebwoods.org/popup.php?lang=ru>), посвященную вопросам обеспечения безопасности в Интернете.

В основной школе учащиеся активно начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайновые игры и так далее. Все более часто их любимым способом общения становится мгновенный обмен сообщениями. Для учащихся этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Педагогам для обеспечения интернет-безопасности учащихся 10-15 лет необходимо:

* познакомить учащихся с ответственным, достойным поведением в Интернете;
* рассказать об основных опасностях и правилах безопасного использования сети Интернет;
* убедить никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете;
* объяснить опасность личных встреч с друзьями по Интернету без присутствия взрослых;
* убедить сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им.
* ознакомь с правилами поведения на форумах и чатах, убедить их, что они не должны использовать сеть для хулиганства, распространения сплетен или угроз другим людям.

Организуя работу с учащимися старших классов по безопасному использованию информации в Интернете, следует обратить внимание на неформальные молодежные объединения, которые возникают в образовательной организации. Сетевая безопасность подростков – трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее, участие взрослых тоже необходимо:

* Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.
* Интересуйтесь, какими чатами и досками объявлений пользуются подростки, и с кем они общаются. Поощряйте использование модерируемых (контролируемых) чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме.
* Настаивайте, чтобы подростки осторожно соглашались или не соглашались вовсе на личные встречи с друзьями из Интернета. Напоминайте, какие опасности это может за собой повлечь.
* Убедите подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.
* Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
* Обсудите с подростками азартные сетевые игры и связанный с ними риск.

Результатами мероприятий по безопасному использованию Интернета могут стать как бумажные, так и электронные ресурсы, созданные учащимися: рисунки, сочинения (рассказы, сказки, стихи), буклеты, презентации. Интересной формой представления результатов могут стать театрализованные выступления и видеофильмы учащихся.

Для учащихся старших классов при создании материалов по безопасности можно использовать сервисы Интернета для совместной деятельности. Работа команды учащихся в этом случае можем проводиться дистанционно. Одним из примеров является схема «Безопасность детей в Интернете». <http://www.mindmeister.com/ru/12485180/>

Рекомендуем обратить внимание на создание условия для ознакомления с результатами творчества учащихся. Разработанные материалы можно размещать на сайте образовательной организации, в социальных сетях, блогах и сетевых сообществах.

Для эффективной профилактики интернет-зависимости, профилактики националистических проявлений в молодежной среде и устранения риска вовлечения подростков в противоправную деятельность педагогам необходимо проводить разъяснительную и консультационную работу с родителями учащихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в Интернет.

Возможно проведение бесед о работе учащихся в сети Интернет на классных и общешкольных родительских собраниях или при индивидуальных встречах; информирование через школьный сайт на страничке для родителей. На таких страничках можно разместить рекомендации по профилактике компьютерной зависимости у детей, по обеспечению безопасности детей в Интернете.

Примеры подобных страничек для родителей:

<http://borovoeshc.ucoz.ru/load/shkola_bezopasnosti/bezopasnyj_internet_dlja_detej/7-1-0-109>— школьный сайт МКОУ Боровская ООШ, о программах родительского контроля.

<http://nsportal.ru/site/112423/bezopasnyy-internet>школьный сайт [МБОУ «Кипринская](http://nsportal.ru/site/112423) [СОШ» Алтайский край](http://nsportal.ru/site/112423), статьи, советы родителям.

Эффективной мерой является установка на компьютер программного обеспечения с функциями «родительского контроля». Родителям можно порекомендовать установить на домашнем компьютере бесплатную программу «Интернет Цензор [www.icensor.ru](http://icensor.ru/).

Родителям могут быть даны следующие рекомендации по формированию у учащихся навыков безопасного поведения в сети Интернет:

* Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.
* Научите детей не загружать программы, музыку или файлы без вашего разрешения.
* Позволяйте заходить на детские сайты только с хорошей репутацией и контролируемым общением.
* Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
* Приучите детей сообщать вам, если что-либо или кто-либо в сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

Единство родительских и педагогических усилий поможет оптимально использовать «плюсы» и нейтрализовать «минусы» работы с ресурсами всемирной Сети.

**Нормативная** **правовая** **база**

* Указ Президента Российской Федерации от 06.12 № 761 «О национальной стратегии действий в интересах детей на 2012-2017 годы».
* Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее — Федеральный закон № 436-ФЗ).
* Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»).
* Федеральный закон от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно- телекоммуникационных сетях.
* Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» ст.
* Письмо Министерства образования и науки РФ от 12.13 № НТ- 1338/08.

**Интернет-ресурсы для педагогических работников**:

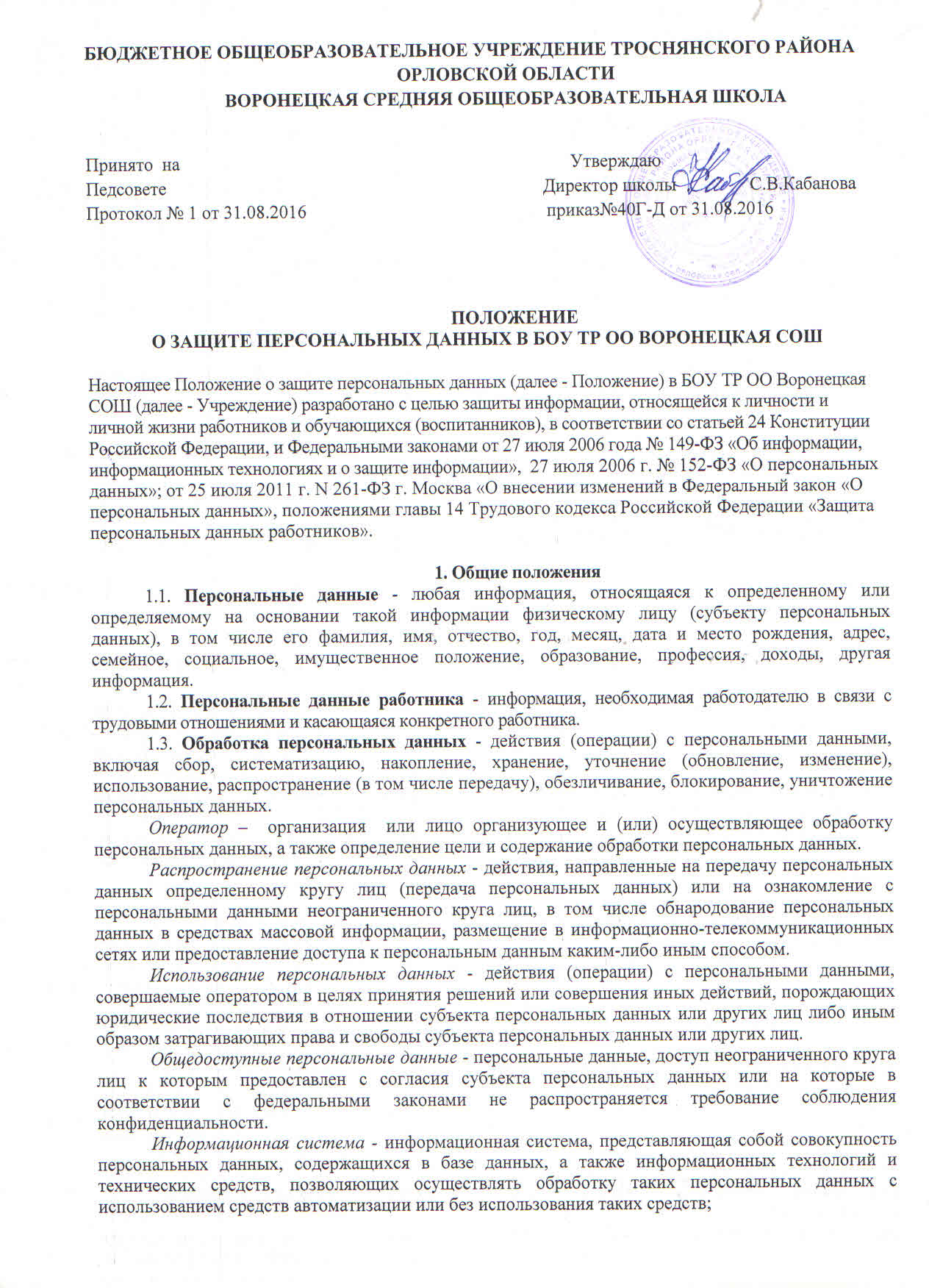
* <http://www.fid.su/projects/deti-v-internete>сайт Фонда Развития Интернет.
* <http://content-filtering.ru/>сайт «Ваш личный интернет», советы, рекомендации для детей и родителей по безопасной работе в Интернет.
* <http://www.ligainternet.ru/>Лиги безопасного Интернета.
* <http://ppt4web.ru/informatika/bezopasnyjj-internet.html>презентации о безопасном Интернете.
* <http://www.microsoft.com/ru-ru/security/default.aspx>сайт Центра безопасности Майкрософт.
* <http://www.saferunet.org/children/>Центр безопасности Интернета в России.
* [https://edu.tatar.ru/upload/images/files/909\_029%20Orangepdf](https://edu.tatar.ru/upload/images/files/909_029%20Orange7.pdf)Безопасно и просто: родительский контроль. — Буклет
* Урок в 9–10 классах. Профилактика интернет-зависимости «Будущее начинается сегодня» [http://festival.1september.ru/articles/612789/](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&amp;url=http%3A%2F%2Ffestival.1september.ru%2Farticles%2F612789%2F)Материал разработан для учащихся 9-11 классов, но может модифицироваться и для учащихся среднего звена школы.
* Материалы (буклет, презентация и текст) для бесед профилактике игровой и интернет-зависимости у детей и подростков на сайте Министерства образования и науки Республики Татарстан: [http://mon.tatarstan.ru/prof\_internet\_zavisimosti.htm](https://docviewer.yandex.ru/r.xml?sk=0c02c71819619c959a25742d60574947&amp;url=http%3A%2F%2Fmon.tatarstan.ru%2Fprof_internet_zavisimosti.htm)
* <http://www.nachalka.com/node/950>Видео «Развлечение и безопасность в Интернете»
* <http://i-deti.org/>портал «Безопасный инет для детей», ресурсы, рекомендации, комиксы
* [http://сетевичок.рф/](http://xn--b1afankxqj2c.xn--p1ai/)сайт для детей — обучение и онлайн-консультирование по вопросам кибербезопасности сетевой безопасности
* <http://www.igra-internet.ru/>— онлайн интернет-игра «Изучи Интернет – управляй им»
* <http://www.safe-internet.ru/>— сайт Ростелеком «Безопасноть детей в Интернете, библиотека с материалами, памятками, рекомендациями по возрастам

# информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников

<http://www.ligainternet.ru/news/> мероприятия Лиги безопасного интернета. Лига безопасного интернета — крупнейшая и наиболее авторитетная в России организация, созданная для противодействия распространению опасного контента во всемирной сети. Лига безопасного интернета была учреждена в 2011 году при поддержке Минкомсвязи РФ, МВД РФ, Комитета Госдумы РФ по вопросам семьи женщин и детей. Попечительский совет Лиги возглавляет помощник Президента Российской Федерации Игорь Щеголев.

<http://xn--b1afankxqj2c.xn--p1ai/partneram-o-proekte> мероприятия проекта «Сетевичок». Проект представляет собой группу онлайн-мероприятий:

* Международный квест по цифровой грамотности «Сетевичок», ориентированный на детей и подростков.
* Национальная премия за заслуги компаний и организаций в сфере информационного контента для детей, подростков и молодежи «Премия Сетевичок»
* Всероссийское исследование детей и подростков «Образ жизни российских подростков в сети».
* Конференция по формированию детского информационного пространства «Сетевичок»

**** 1.4. К персональным данным работника Учреждения, получаемым работодателем и подлежащим хранению у работодателя в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах работников:

- паспортные данные работника;

– ИНН;

- копия страхового свидетельства государственного пенсионного страхования;

- копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

- копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);

- анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);

- документы о возрасте малолетних детей и месте их обучения;

- документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);

- документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);

- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);

- трудовой договор;

- заключение по данным психологического исследования (если такое имеется);

- копии приказов о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;

- личная карточка по форме Т-2;

- заявления, объяснительные и служебные записки работника;

- документы о прохождении работником аттестации, повышения квалификации;

- иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником (включая приговоры суда о запрете заниматься педагогической деятельностью или занимать руководящие должности).

1.5. К персональным данным обучающихся (воспитанников) Учреждения, получаемыми и подлежащим хранению в Учреждении в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в информационной системе Учреждения:

– документы, удостоверяющие личность обучающегося (свидетельство о рождении или паспорт);

– документы о месте проживания;

– документы о составе семьи;

– паспортные данные родителей (законных представителей) обучающегося;

– документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.);

– иные документы, содержащие персональные данные (в том числе сведения, необходимые для предоставления обучающемуся (его родителям, законным представителям) гарантий и компенсаций, установленных действующим законодательством).

**2. Основные условия проведения обработки персональных данных**

2.1. Учреждение определяет объем, содержание обрабатываемых персональных данных работников и обучающихся, руководствуясь Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Законом РФ «Об образовании» и иными федеральными законами.

2.2. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, а также обеспечения личной безопасности работников, сохранности имущества, контроля количества и качества выполняемой работы.

Обработка персональных данных обучающихся (воспитанников) Учреждения может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов; содействия обучающимся в обучении, обеспечения их личной безопасности; контроля качества обучения и обеспечения сохранности имущества.

2.3. Все персональные данные работника Учреждения предоставляются работником, за исключением случаев, предусмотренных федеральным законом. Если персональные данные работника возможно получить только у третьей стороны, то работодатель обязан заранее уведомить об этом работника и получить его письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

2.4. Работники и родители (законные представители) обучающегося (воспитанника) должны быть проинформированы о целях обработки персональных данных.

2.5. Учреждение не имеет права получать и обрабатывать персональные данные работника, обучающегося (воспитанника) о его политических, религиозных и иных убеждениях и частной жизни без письменного согласия работника, обучающегося (воспитанника).

Учреждение не имеет права получать и обрабатывать персональные данные работника, обучающегося (воспитанника) о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

2.6. Учреждение вправе осуществлять сбор, передачу, уничтожение, хранение, использование информации о политических, религиозных, других убеждениях и частной жизни, а также информации, нарушающей тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений:

– работника только с его письменного согласия или на основании судебного решения.

– обучающегося (воспитанника) только с его письменного согласия (согласия родителей (законных представителей) малолетнего несовершеннолетнего обучающегося, воспитанника) или на основании судебного решения.

**3. Хранение и использование персональных данных**

3.1. Персональные данные хранятся на бумажных и электронных носителях, в специально предназначенных для этого помещениях.

**3.2.** В процессе хранения персональных данных должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;

- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

3.3. Доступ к персональным данным работников образовательное учреждение имеют:

- директор;

- главный бухгалтер;

- иные работники, определяемые приказом директора Учреждения, в пределах своей компетенции.

3.4. Доступ к персональным данным учащихся, родителей имеют следующие должностные лица, непосредственно использующие их в служебных целях:

а) директор Учреждения;

г) педагоги

3.5. Уполномоченные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

Все остальные работники, учащиеся имеют право на полную информацию только об их персональных данных и обработке этих данных.

3.6. Должностные лица, использующие персональные данные должны подписать обязательство о неразглашении конфиденциальной информации персональных данных.

3.7. Получение сведений о персональных данных работников, учащихся третьей стороной разрешается только при наличии заявления с указанием конкретных персональных данных и целей, для которых они будут использованы, а также письменного согласия работника, обучающегося персональные данные которого затребованы.

3.8. Получение персональных данных работника, учащегося третьей стороной без его письменного согласия возможно в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровья работника, учащегося, а также в случаях, установленных законом. Письменное согласия субъекта персональных данных на получение, обработку, хранение и передачу третьим лицам сведений, относящихся к персональным данным, закрепляется в договоре на оказание услуг.

3.9. Внешний доступ (другие организации и граждане).

Сообщение сведений о персональных данных работников, учащихся другим организациям и гражданам разрешается при наличии письменного согласия работника, обучающегося и заявления подписанного руководителем организации либо гражданином, запросившим такие сведения.

3.10. Предоставление сведений о персональных данных работников, учащихся без соответствующего их согласия возможно в следующих случаях:

а) в целях предупреждения угрозы жизни и здоровья работника, обучающегося;

б) при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;

в) при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов, отдела по делам несовершеннолетних, отдела опеки и попечительства.

Получателями персональных данных работника на законном основании являются:

1) органы социального страхования, органы пенсионного обеспечения, а также иные органы, организации и граждане (в соответствии с Федеральным законом от 16.07.1999 № 165-ФЗ "Об основах обязательного социального страхования", согласно которому отношения по обязательному социальному страхованию возникают у страхователя (работодателя) – по всем видам обязательного социального страхования с момента заключения с работником трудового договора);

2) налоговые органы (в соответствии со ст. 24 Налогового кодекса РФ, выступая в качестве налогового агента работников, исчисляющего, удерживающего из средств, выплачиваемых работникам, и перечисляющего в бюджет соответствующие налоги, работодатель обязан представлять в налоговый орган по месту своего учета документы, необходимые для контроля за правильностью исчисления, удержания и перечисления налогов);

3.11. Помимо лиц, указанных в п. 3.3. настоящего Положения, право доступа к персональным данным имеют только лица, уполномоченные действующим законодательством.

3.12. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные лишь в целях, для которых они были предоставлены.

3.13. Ответственным за организацию и осуществление хранения персональных данных работников и обучающихся Учреждения является сотрудник, организующий кадровую работу и делопроизводство в соответствии с приказом директора.

3.14. Персональные данные работников отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в специально оборудованных несгораемых шкафах в алфавитном порядке.

3.15. Персональные данные работников и обучающихся (воспитанников) содержатся в информационной системе Учреждения на бумажных носителях и в электронном виде. Персональные данные на бумажных носителях формируются и хранятся в порядке, определенном номенклатурой дел Учреждения.

**4. Передача персональных данных**

4.1. При передаче персональных данных другим юридическим и физическим лицам Учреждение должно соблюдать следующие требования:

4.1.1. Персональные данные работника (обучающегося, воспитанника) не могут быть сообщены третьей стороне без письменного согласия работника, обучающегося (воспитанника), родителей (законных представителей) обучающегося (воспитанника), за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника (обучающегося, воспитанника), а также в случаях, установленных федеральным законом.

4.1.2. Лица, получающие персональные данные работника (обучающегося, воспитанника) должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Учреждение должно требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами.

4.2. Передача персональных данных работника (обучающегося, воспитанника) его представителям может быть осуществлена в установленном действующим законодательством порядке только в том объеме, который необходим для выполнения указанными представителями их функций.

**5. Права работников, обучающихся (воспитанников) на обеспечение защиты персональных данных**

5.1. В целях обеспечения защиты персональных данных, хранящихся в Центре, работники и обучающиеся (родители (законные представители) несовершеннолетнего обучающегося), имеют право:

5.1.1. Получать полную информацию о своих персональных данных и их обработке.

5.1.2. Свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении работника, обучающегося (его родителей, законных представителей) – к лицу, ответственному за организацию и осуществление хранения персональных данных работников.

5.1.3. Требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением работника на имя директора Учреждения.

При отказе директора Учреждения исключить или исправить персональные данные работника работник, обучающийся (родитель, законный представитель несовершеннолетнего обучающегося) имеет право заявить в письменном виде директору Учреждения о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник, обучающийся (родитель, законный представитель несовершеннолетнего обучающегося) имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.1.4. Требовать об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обучающегося (воспитанника) обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.1.5. Обжаловать в суде любые неправомерные действия или бездействия при обработке и защите его персональных данных.

**6. Обязанности субъекта персональных данных по обеспечению достоверности его персональных данных**

6.1. В целях обеспечения достоверности персональных данных работники обязаны:

6.1.1. При приеме на работу в Учреждение представлять уполномоченным работникам Учреждения достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

6.1.2. В случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) и т.п. сообщать об этом в течение 5 рабочих дней с даты их изменений.

**7. Ответственность за нарушение настоящего положения**

7.1. За нарушение порядка обработки (сбора, хранения, использования, распространения и защиты) персональных данных должностное лицо несет административную ответственность в соответствии с действующим законодательством.

7.2. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

7.3. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

7.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников, обучающихся, родителей, привлекаются к дисциплинарной ответственности. К данным лицам могут быть применены следующие дисциплинарные взыскания:

а) замечание;

б) выговор;

в) предупреждение о неполном должностном соответствии;

г) освобождение от занимаемой должности;

д) увольнение.

Директор Учреждения может расторгнуть трудовой договор по своей инициативе по подп. "в" п. 6 ч. 1 ст. 81 ТК РФ при разглашении должностным лицом охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в т. ч. в случае разглашения персональных данных другого работника.

7.5. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

7.6. Копия приказа о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.

7.7. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

7.8. Учреждение вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

– относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);

– полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных (обучающийся и др.), если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

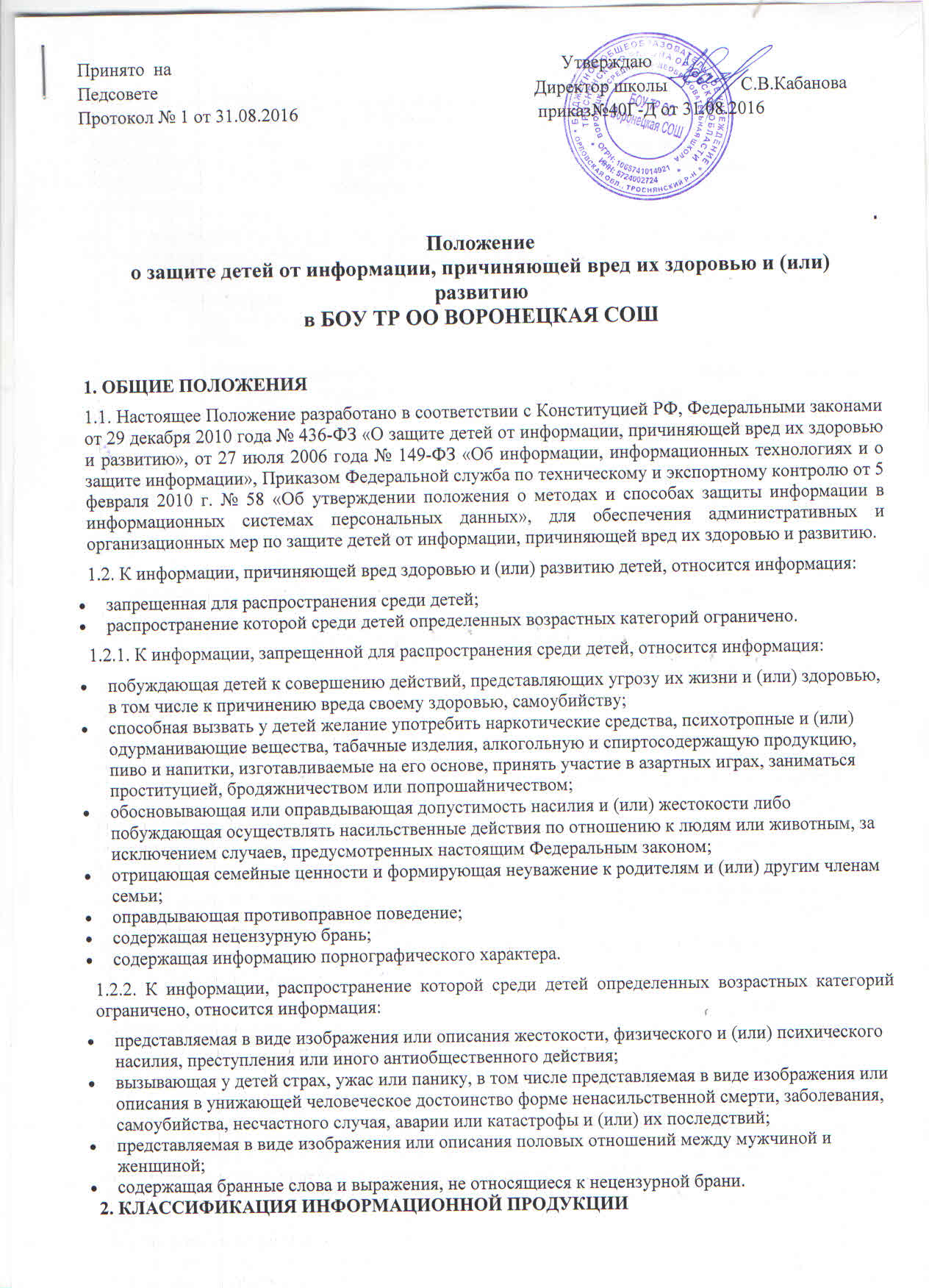
– являющихся общедоступными персональными данными;

– включающих в себя только фамилии, имена и отчества субъектов персональных данных;

– включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

– обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Во всех остальных случаях оператор (директор центра и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

2.1. Классификация информационной продукции осуществляется по следующим категориям:

* информационная продукция для детей, не достигших возраста шести лет;
* информационная продукция для детей в возрасте от шести до двенадцати лет;
* информационная продукция для детей в возрасте от двенадцати до шестнадцати лет;
* информационная продукция для детей в возрасте от шестнадцати до восемнадцати лет;
* информационная продукция, запрещенная для распространения среди детей (п. 1.2.1. настоящего Положения).

2.1.1. К информационной продукции для детей, не достигших возраста шести лет, может быть отнесена информационная продукция, содержащая информацию, не причиняющую вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные ее жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия).

2.1.2. К информационной продукции для детей в возрасте от шести до двенадцати лет, может быть отнесена информационная продукция, предусмотренная п.2.1.1. настоящего Положения, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

* кратковременные и ненатуралистические изображение или описание заболеваний человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого достоинства;
* ненатуралистические изображение или описание несчастного случая, аварии, катастрофы либо ненасильственной смерти без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику;
* не побуждающие к совершению антиобщественных действий и (или) преступлений эпизодические изображение или описание этих действий и (или) преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим.

2.1.3. К информационной продукции для детей в возрасте от двенадцати до шестнадцати лет, может быть отнесена информационная продукция, предусмотренная п. 2.1.2.настоящего Положения, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

* эпизодические изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);
* изображение или описание, не побуждающие к совершению антиобщественных действий (в том числе к потреблению алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на его основе, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий;
* не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

2.1.4. К информационной продукции для детей в возрасте от шестнадцати до восемнадцати лет, может быть отнесена информационная продукция, предусмотренная п. 2.1.3. настоящего Положения, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

* изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий, которые могут вызывать у детей страх, ужас или панику;
* изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);
* информация о наркотических средствах или о психотропных и (или) об одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления;
* отдельные бранные слова и (или) выражения, не относящиеся к нецензурной брани;
* не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

**3. ДЕЯТЕЛЬНОСТЬ ОУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ**

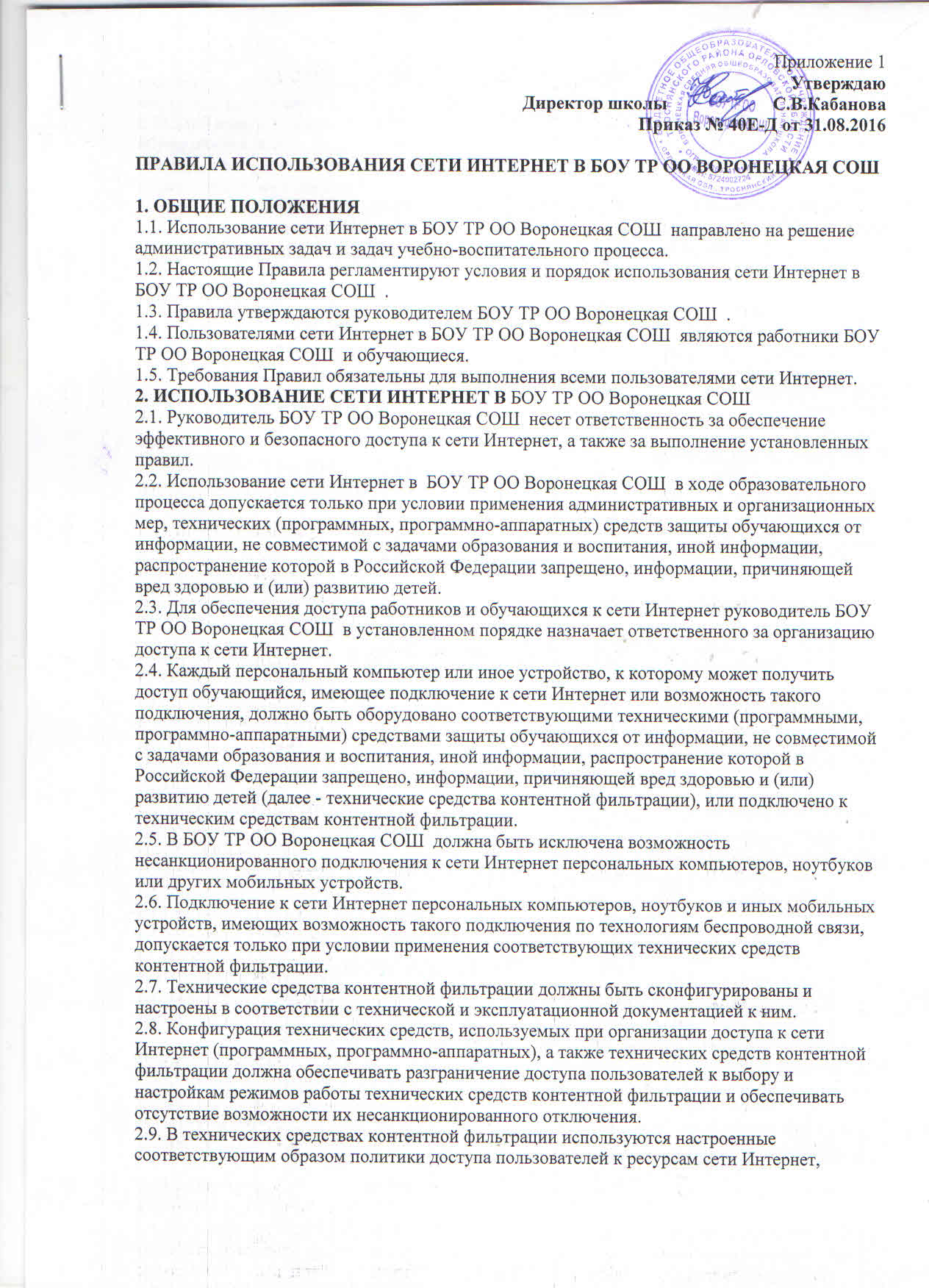
3.1.5. График работы точек доступа к сети Интернет и список ответственных лиц устанавливается приказом по школе.

3.1.6. Обеспечение технических и программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и развитию в точках коллективного доступа к сети Интернет осуществляется работниками школы в соответствии с их должностными обязанностями.

3.1.7. Контроль за соответствием содержания и художественного оформления печатных изданий, полиграфической продукции (в том числе тетрадей, дневников, обложек для книг, закладок для книг), аудиовизуальной продукции, иной информационной продукции, используемой в образовательном процессе требованиям, предъявляемым к информационной продукции для детей соответствующей возрастной группы осуществляется работниками школы в соответствии с их должностными обязанностями.

**4. ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ЗАЩИТЫ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ**

4.1. Нарушение законодательства РФ о защите детей от информации, причиняющей вред их здоровью и развитию, влечет за собой ответственность в соответствии с действующим законодательством РФ.

исключающие доступ обучающихся к информации, не совместимой с задачами образования и воспитания, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей.  
2.10. При использовании ресурсов сети Интернет в БОУ ТР ОО Воронецкая СОШ обучающимся может предоставляться доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу.  
2.11. Перечень ресурсов сети Интернет, разрешенных для использования в образовательном процессе обучающимися, или ресурсов сети Интернет, противоречащих задачам образования и воспитания, определяется политиками доступа, применяемыми в технических средствах контентной фильтрации.  
2.12. Установка, конфигурация, настройка режимов работы технических средств контентной фильтрации, а также применение в технических средствах контентной фильтрации политик доступа к ресурсам сети Интернет и другие технические меры, определенные пунктами 2.4 - 2.11 настоящих Правил, осуществляются работником БОУ ТР ОО Воронецкая СОШ , назначенным ответственным за организацию доступа к сети Интернет в соответствии с пунктом 2.3 настоящих Правил, или иным назначаемым в установленном порядке работником БОУ ТР ОО Воронецкая СОШ .  
К проведению работ, связанных с установкой, конфигурацией, настройкой режимов работы и эксплуатацией технических средств контентной фильтрации, может привлекаться сторонняя организация на основании заключаемого между БОУ ТР ОО Воронецкая СОШ и сторонней организацией договора.  
2.13. Использование сети Интернет работниками БОУ ТР ОО Воронецкая СОШ допускается только в целях исполнения ими своих должностных обязанностей и в целях образовательного процесса, использование сети Интернет обучающимися допускается только в целях образовательного процесса.  
2.14. Использование сети Интернет в БОУ ТР ОО Воронецкая СОШ в личных целях работниками и обучающимися не допускается.  
2.15. В процессе использования обучающимися сети Интернет , педагогами БОУ ТР ОО Воронецкая СОШ осуществляется контроль использования технических средств, применяемых при организации доступа к сети Интернет (программных, программно-аппаратных), в том числе контроль функционирования технических средств контентной фильтрации, а также контроль доступа обучающихся к ресурсам сети Интернет.  
2.16. В целях своевременного выявления угроз, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, в БОУ ТР ОО Воронецкая СОШ проводится периодический контроль состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет, в том числе контроль функционирования технических средств контентной фильтрации.  
Периодичность такого контроля и состав мероприятий по контролю устанавливается руководителем БОУ ТР ОО Воронецкая СОШ .

**3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ**  
3.1. Пользователям сети Интернет запрещается:  
осуществлять поиск, получение информации, распространение которой на территории Российской Федерации запрещено, иной информации, содержание которой является не совместимым с задачами образования и воспитания (эротика, порнография, наркомания, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иная информация схожей направленности); обращаться к ресурсам сети Интернет, содержащим такую информацию;  
осуществлять любые сделки через сеть Интернет;  
распространять в сети Интернет оскорбительную, не соответствующую действительности и (или) порочащую других лиц информацию, угрозы жизни, здоровью, иную информацию, распространение которой на территории Российской Федерации запрещено;  
осуществлять любые действия, направленные на получение несанкционированного доступа к сети Интернет;  
осуществлять любые действия, направленные на вмешательство в функционирование технических средств контентной фильтрации доступа к сети Интернет.  
**3.2. Обучающийся:**в случае выявления наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, незамедлительно информирует преподавателя, ведущего занятие, или иного ответственного работника БОУ ТР ОО Воронецкая СОШ .

3.3. Педагог, ведущий занятие, иной ответственный работник БОУ ТР ОО Воронецкая СОШ обязан:  
осуществлять постоянный контроль использования технических средств, применяемых при организации доступа к сети Интернет (программных, программно-аппаратных), в том числе контроль функционирования технических средств контентной фильтрации, а также контроль доступа обучающихся к ресурсам сети Интернет; при получении информации от обучающихся о получении доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, или в случае самостоятельного выявления наличия доступа к таким ресурсам сети Интернет, незамедлительно принимать меры, направленные на прекращение и ограничение доступа обучающихся к такой информации, а также информировать об инциденте работника БОУ ТР ОО Воронецкая СОШ , ответственного за организацию доступа к сети Интернет.

**4. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ**  
4.1. В силу особенностей информационных технологий, применяемых в сети Интернет, технические средства контентной фильтрации, установленные в БОУ ТР ОО Воронецкая СОШ в соответствии с технической и эксплуатационной документацией к ним и в соответствии с настоящими Правилами, не могут гарантировать обеспечение полного и всестороннего ограничения доступа к информации, не совместимой с задачами образования и воспитания, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей.  
4.2. Преподаватель, ведущий занятие, иной ответственный работник БОУ ТР ОО Воронецкая СОШ в порядке реагирования на инцидент, связанный с обнаружением факта доступности ресурсов сети Интернет, содержащих информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, при информировании работника, ответственного за организацию доступа к сети Интернет, сообщает о наличии доступа к конкретному ресурсу сети Интернет и точном адресе его размещения (URL).  
4.3. Работник, ответственный за организацию доступа к сети Интернет, при получении информации, указанной в пункте 4.2 настоящих Правил, принимает следующие меры:  
устанавливает обстоятельства получения доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей;  
идентифицирует ресурс сети Интернет;  
в течение одного рабочего дня с момента получения информации, указанной в п. 4.2 настоящих Правил, проводит мероприятия, направленные на ограничение доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей (вносит изменения в политики доступа, применяемые в технических средствах контентной фильтрации, вносит изменения в конфигурацию технических средств контентной фильтрации, в случае необходимости предпринимает другие меры).  
4.4. Работник, ответственный за организацию доступа к сети Интернет, проводит анализ обстоятельств, послуживших причиной доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.  
4.5. В течение пяти рабочих дней с момента получения информации, указанной в п. 4.2 настоящих Правил работник, ответственный за организацию доступа к сети Интернет, вносит руководителю БОУ ТР ОО Воронецкая СОШ на основе проведенного анализа предложения по совершенствованию системы контентной фильтрации в целях минимизации количества инцидентов, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.  
4.6. В порядке реагирования на инцидент образовательной организацией может быть дополнительно направлено сообщение о наличии на страницах сайтов в сети Интернет информации, распространение которой в Российской Федерации запрещено:  
4.6.1. В Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций путем заполнения соответствующей электронной формы, размещенной в сети Интернет по адресу http://eais.rkn.gov.ru/feedback/ в случае выявления:  
информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, а также о способах и местах культивирования наркосодержащих растений;  
информации о способах совершения самоубийства, а также призывов к совершению самоубийства;  
материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;  
иной информации, решение о запрете распространения которой на территории Российской Федерации принято уполномоченными органами или судом.  
4.6.2. В Министерство внутренних дел в случае выявления материалов экстремистского характера.  
4.7. Сообщение о наличии на страницах сайтов в сети Интернет информации, распространение которой в Российской Федерации запрещено, образовательной организацией может быть также направлено:  
в Управление Федеральной службы по контролю за оборотом наркотиков России в случае выявления информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, а также о способах и местах культивирования наркосодержащих растений;  
в Управление Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека в случае выявления информации о способах совершения самоубийства, а также призывов к совершению самоубийства;  
в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в случае выявления материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера, иной информации, решение о запрете распространения которой на территории Российской Федерации принято уполномоченными органами или судом.  
4.8. Направление БОУ ТР ОО Воронецкая СОШ в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерство внутренних дел, территориальные органы федеральных органов государственной власти, указанные в пункте 4.7 настоящих Правил, сообщения о наличии на страницах сайтов в сети Интернет информации, распространение которой в Российской Федерации запрещено, подтверждается документально в соответствии с установленными в образовательной организации требованиями к оформлению служебных документов.  
4.9. В ходе работ по реагированию на инциденты, связанные с выявлением ресурсов сети Интернет, содержащих материалы экстремистского характера, образовательная организация руководствуется Федеральным списком экстремистских материалов Министерства юстиции Российской Федерации, размещенным в сети Интернет по адресу: http://minjust.ru/ru/extremist-materials.

**5. ОТВЕТСТВЕННОСТЬ**

5.1. При организации доступа и использовании сети Интернет в БОУ ТР ОО Воронецкая СОШ педагоги несут персональную ответственность в соответствии действующим законодательством Российской Федерации.  
5.2. Обучающиеся и их родители (законные представители) несут ответственность за неправомерное использование сети Интернет в порядке, установленном в БОУ ТР ОО Воронецкая СОШ , и в соответствии с действующим законодательством Российской Федерации.

**ПЛАН МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ ПРИ ОРГАНИЗАЦИИ ДОСТУПА К СЕТИ ИНТЕРНЕТ**

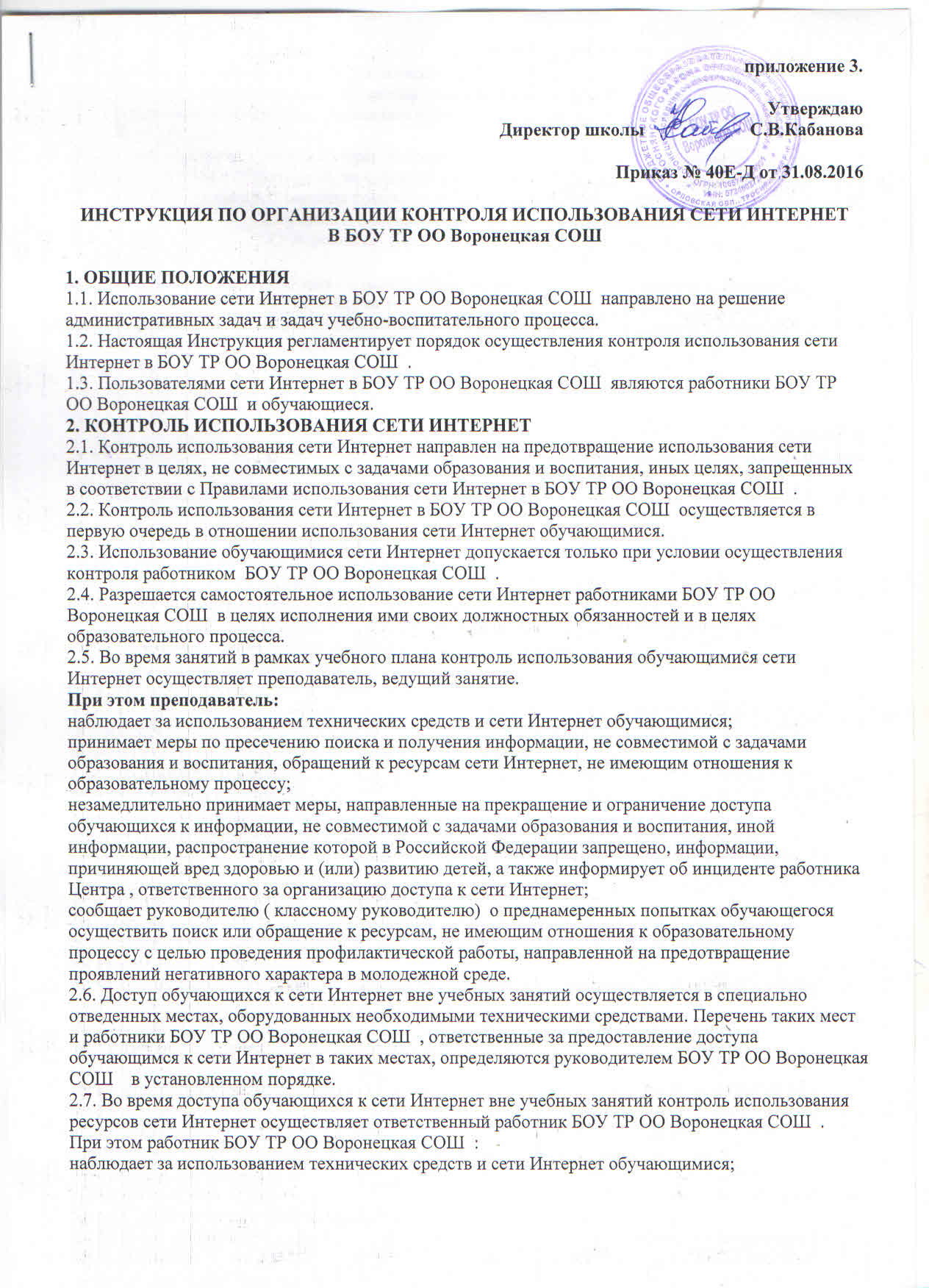
Приложение 1  
к Правилам  
использования сети Интернет  
в БОУ ТР ОО Воронецкая СОШ

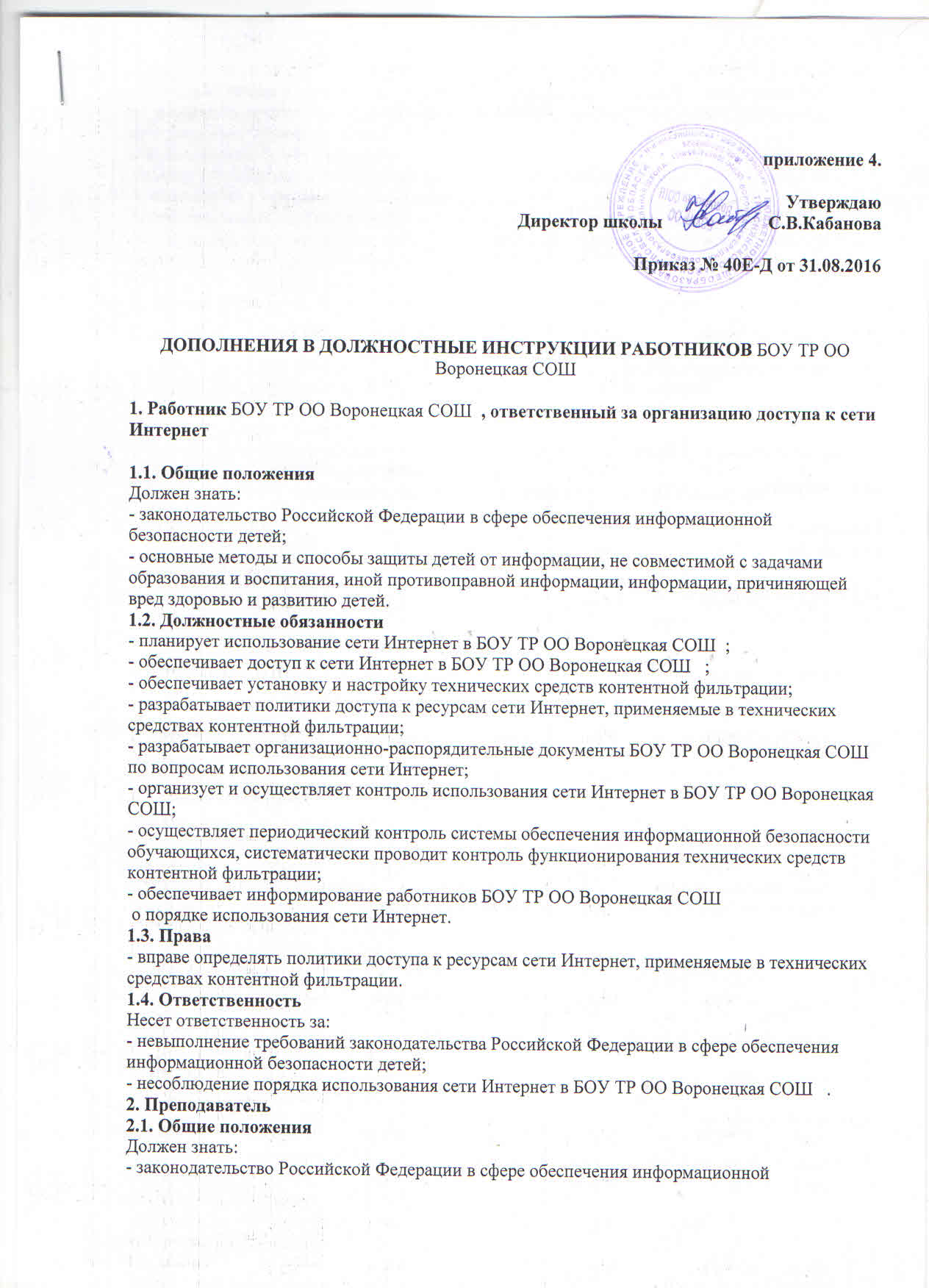
|  |  |  |
| --- | --- | --- |
|  |  |  |
| N  п/п | Мероприятие | Сроки |
| 1. | Издание (актуализация) организационно-распорядительных документов по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет | январь |
| 2. | Заключение договора с оператором связи на оказание услуг доступа к сети Интернет с контентной фильтрацией | Декабрь -  январь |
| 3. | Настройка (установка) технических средств, применяемых при организации доступа к сети Интернет (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) в соответствии с требованиями организационно-распорядительных документов по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет | январь |
| 4. | Установка, конфигурация, настройка режимов работы технических средств контентной фильтрации | Январь- февраль |
| 5. | Внесение изменений в политики доступа к ресурсам сети  Интернет, применяемые в технических средствах контентной фильтрации | По мере  необходимости, в порядке  реагирования  на инцидент |
| 6. | Информирование работников БОУ ТР ОО Воронецкая СОШ о необходимости соблюдения требований законодательства Российской Федерации и организационно-распорядительных документов БОУ ТР ОО Воронецкая СОШ по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет | январь |
| 7. | Информирование работников образовательной организации, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации и организационно-распорядительных документов БОУ ТР ОО Воронецкая СОШ по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет | Январь- февраль |
| 8. | Информирование родителей (законных представителей) обучающихся о существующих угрозах в сети Интернет, о методах и способах защиты детей от информации, причиняющей вред здоровью и (или) развитию детей | Февраль- апрель |
| 9. | Проведение периодического контроля состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет | Сентябрь |

Приложение 2  
к Правилам  
использования сети Интернет  
в БОУ ТР ОО Воронецкая СОШ

**ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ ПО КОНТРОЛЮ СОСТОЯНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ ПРИ ОРГАНИЗАЦИИ ДОСТУПА К СЕТИ ИНТЕРНЕТ**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| N  п/п | Мероприятие | Периодичность |
| 1. | Анализ организационно-распорядительных документов по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет на предмет наличия необходимых документов и их актуальности | Не реже 1  раза в год |
| 2. | Проверка соблюдения работниками БОУ ТР ОО Воронецкая СОШ обязанностей, предусмотренных Правилами использования сети Интернет в образовательной организации, должностной инструкцией | Не реже 1  раза в год |
| 3. | Текущий контроль эксплуатации технических средств контентной фильтрации | Постоянно |
| 4. | Контроль функционирования технических средств контентной фильтрации и их конфигурации | Не реже 2 раз в год |
| 5. | Контроль организации доступа к сети Интернет в целях исключения возможности несанкционированного использования сети Интернет в образовательной организации | Постоянно |
| 6. | Контроль функционирования технических средств, применяемых при организации доступа к сети Интернет, и их конфигурации (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) | Не реже 2 раз в год |
| 7. | Контроль изменения конфигурации технических средств, применяемых при организации доступа к сети Интернет, контроль наличия в их составе аппаратных, программных средств, предназначенных для нарушения функционирования технических средств контентной фильтрации | Не реже 2 раз в год |
| 8. | Анализ журналов регистрации посещений ресурсов сети Интернет | Не реже 1  раза в месяц |
| 9. | Контроль функционирования системы антивирусной защиты в БОУ ТР ОО Воронецкая СОШ | Не реже 1  раза в месяц |
| 10. | Контроль наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, путем осуществления попыток получения доступа к таким ресурсам сети Интернет | Не реже 4 раз в год |

**** принимает меры по пресечению поиска и получения информации, не совместимой с задачами образования и воспитания, обращений к ресурсам сети Интернет, не имеющим отношения к образовательному процессу;  
незамедлительно принимает меры, направленные на прекращение и ограничение доступа обучающихся к информации, не совместимой с задачами образования и воспитания, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей, а также информирует об инциденте работника БОУ ТР ОО Воронецкая СОШ , ответственного за организацию доступа к сети Интернет;  
сообщает о преднамеренных попытках обучающегося осуществить поиск или обращение к ресурсам, не имеющим отношения к образовательному процессу с целью проведения профилактической работы, направленной на предотвращение проявлений негативного характера в молодежной среде.

****

безопасности детей;  
- основные методы и способы защиты детей от информации, не совместимой с задачами образования и воспитания, иной противоправной информации, информации, причиняющей вред здоровью и развитию детей.

**2.2. Должностные обязанности**

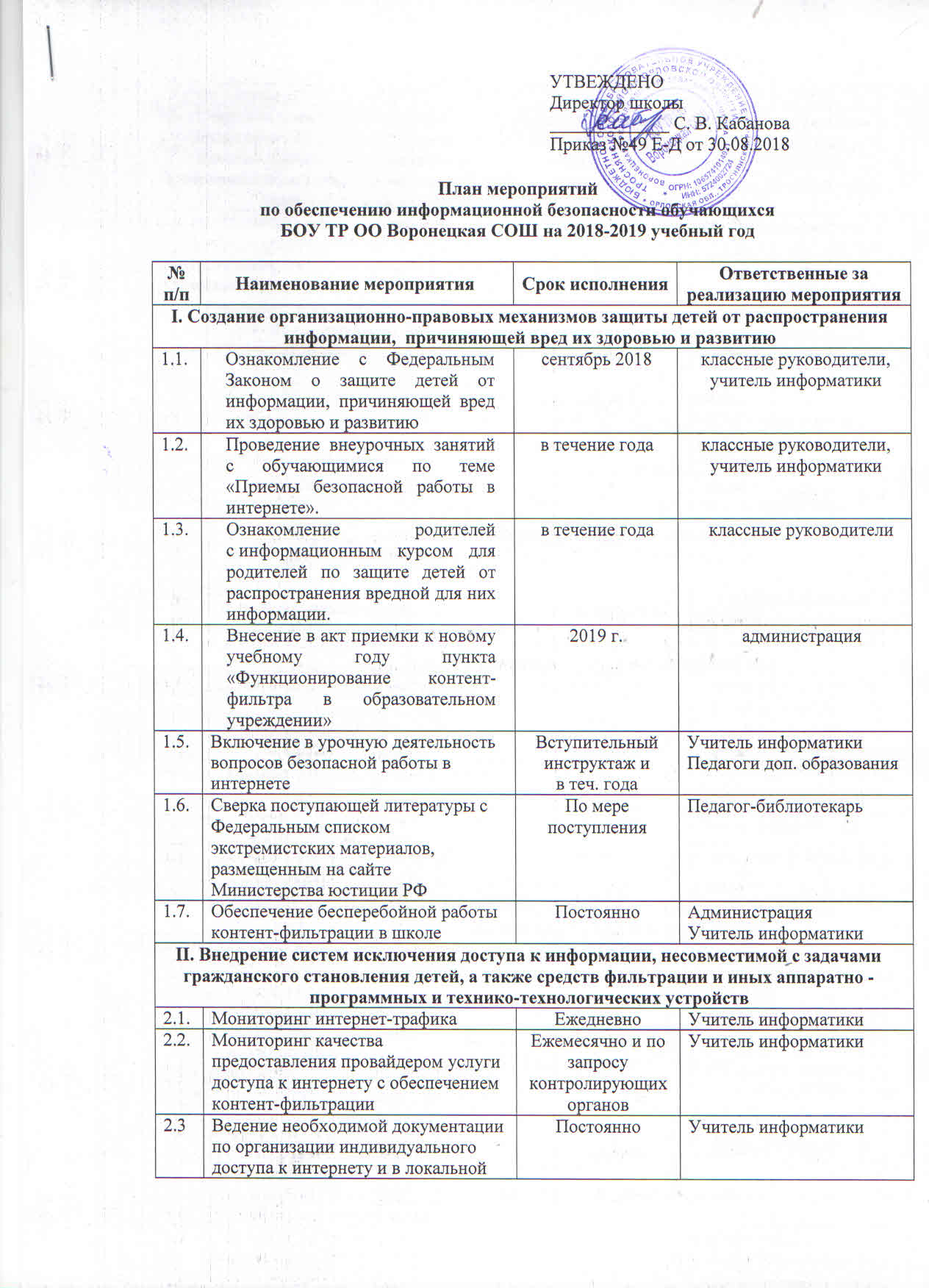
- планирует использование сети Интернет в образовательном процессе с учетом специфики преподаваемого предмета, курса, программы;  
- незамедлительно принимает меры, направленные на прекращение доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, в порядке, установленном правилами использования сети Интернет в БОУ ТР ОО Воронецкая СОШ

**2.3. Права**

- вправе участвовать в разработке и вносить предложения в политики доступа к ресурсам сети Интернет, применяемые в технических средствах контентной фильтрации.

**2.4. Ответственность**

Несет ответственность за:  
- невыполнение требований законодательства Российской Федерации в сфере обеспечения информационной безопасности детей;  
- несоблюдение порядка использования сети Интернет в БОУ ТР ОО Воронецкая СОШ   
.



|  |  |  |  |
| --- | --- | --- | --- |
|  | сети школы |  |  |
| **III. Профилактика у детей и подростков интернет-зависимости, игровой зависимости и правонарушений с использованием информационно- телекоммуникационных технологий, формирование у несовершеннолетних навыков ответственного и безопасного поведения в современной информационно - телекоммуникационной среде через обучение их способам защиты от вредной информации** | | | |
| 3.1. | Проведение мероприятий по теме «Информационная безопасность» | В теч. года | Учитель информатики Классные руководители |
| 3.2. | Проведение ежегодных мероприятий в рамках недели «Интернет-безопасность» для учащихся и их родителей | По плану мероприятий | Учитель информатики Классные руководители |
| 3.3. | Участие в Международном Дне безопасного Интернета | По плану мероприятий | Учитель информатики Классные руководители |
| 3.4. | Участие в обучающих семинарах для руководителей и учителей по созданию надежной системы защиты детей от противоправного контента в образовательной среде школы и дома | По плану мероприятий | Директор  Учитель информатики Педагогические работники |
| 3.5. | Организация индивидуального доступа работников и учащихся к незапрещенным сетевым образовательным ресурсам, в том числе к Дневник.ру | До 15 сентября и по мере необходимости | Учитель информатики |
| 3.6. | Контроль за использованием программно-технических средств, обеспечивающих исключение доступа работников и учащихся к ресурсам интернета, содержащим информацию, несовместимую с образовательной деятельностью школы | Постоянно | Директор  Учитель информатики |
| 3.7. | **Выполнение комплекса мер по антивирусной защите компьютерной техники** | Постоянно | Учитель информатики |
| 3.8. | **Контроль за использованием лицензионного программного обеспечения в административной и образовательной деятельности** | Постоянно | Учитель информатики |
| **IV. Информационное просвещение граждан о возможности защиты детей от информации, причиняющей вред их здоровью и развитию** | | | |
| 4.1. | Участие в различных мероприятиях (лекториях, семинарах, практикумах, тренингах, круглых столах, конференциях и т.п.), в том числе с применением дистанционных технологий, по проблемам информационной безопасности для всех участников образовательных отношений | По плану мероприятий | Учитель информатики Педагогические работники |
| 4.2. | Использование в работе электронных образовательных ресурсов, аккумулирующих сведения о лучших ресурсах для педагогических работников, учащихся и родителей | Постоянно | Учитель информатики Классные руководители |
| 4.3. | Включение вопросов информационной безопасности в административном процессе и образовательной деятельности в повестку совещаний при директоре, на Педагогических советах, в организованных открытых мероприятиях | По плану мероприятий | Директор  Учитель информатики |
| 4.4. | Включение вопросов информационной безопасности в повестку классных часов | Постоянно | Классные руководители |
| 4.5. | Включение вопросов информационной безопасности в повестку родительских собраний | Постоянно | Классные руководители |
| 4.6. | Размещение на официальном сайте информации по информационной безопасности с указанием нормативной документации, ссылок на ресурсы по информационной безопасности в сети интернет и т.п. | По мере необходимости | Учитель информатики |

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;

2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

3. К информации, запрещенной для распространения среди детей, относится:

4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;

5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;

7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

8. оправдывающая противоправное поведение;

9. содержащая нецензурную брань;

10. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.

2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.

3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)

4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).

5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7 - 8 лет

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.

3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.

4. Используйте специальные детские поисковые машины.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.

8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

9. Научите детей не загружать файлы, программы или музыку без вашего согласия.

10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.

11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".

14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.

9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.

13. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

14. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают

общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10.Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

ИНФОРМАЦИОННАЯ ПАМЯТКА

ДЛЯ ОБУЧАЮЩИХСЯ ДЛЯ РАЗМЕЩЕНИЯ

НА ОФИЦИАЛЬНЫХ ИНТЕРНЕТ-РЕСУРСАХ

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;

2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

5. Ограничь физический доступ к компьютеру для посторонних лиц;

6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", который переводится как "беспроводная точность".

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;

3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе;

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;

5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";

6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi автоматически". Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;

3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронная почта

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя\_пользователя@имя\_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный\_фанат@" или "рок2013" вместо "тема13";

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Кибербуллинг или виртуальное издевательство

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;

2. Управляй своей киберрепутацией;

3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;

4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

5. Соблюдай свою виртуальную честь смолоду;

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;

7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

Необходимо обновлять операционную систему твоего смартфона;

Используй антивирусные программы для мобильных телефонов;

Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;

Периодически проверяй, какие платные услуги активированы на твоем номере;

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

В подобных играх стоит опасаться своих соперников, кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

3. Не указывай личную информацию в профайле игры;

4. Уважай других участников по игре;

5. Не устанавливай неофициальные патчи и моды;

6. Используй сложные и разные пароли;

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;

3. Используй сложные и разные пароли. Если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;

5. Установи надежный пароль (PIN) на мобильный телефон;

6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";

3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

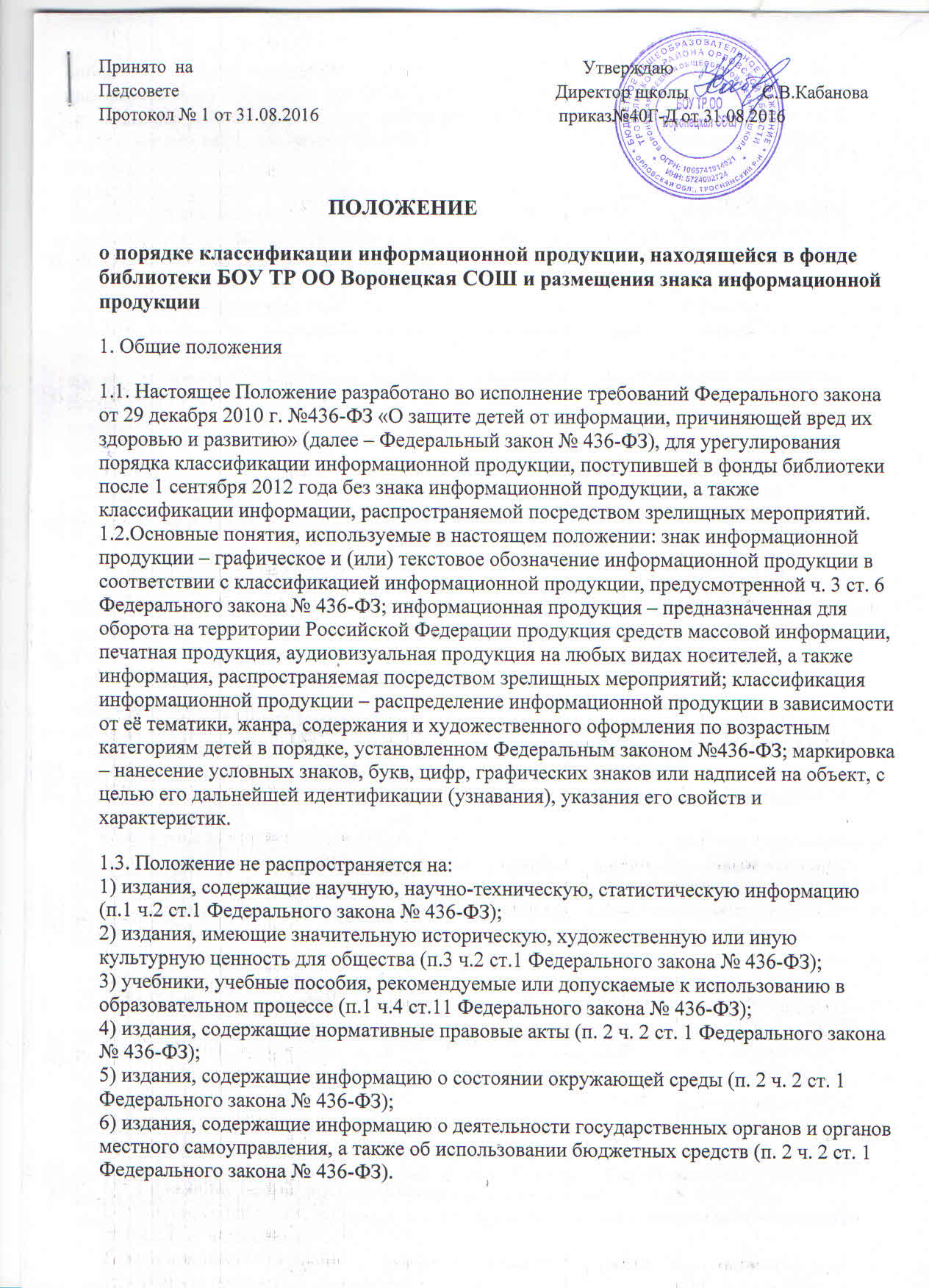
Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

О портале

Сетевичок.рф - твой советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином

Библиотека самостоятельно определяет издания, не маркируемые знаком информационной продукции (п.1 ст. 6 Федерального закона № 436-ФЗ). При определении печатных изданий, не подлежащих классификации и нанесению знака информационной продукции (маркировке), может быть использована Библиотечно-библиографическая классификация - ББК (разделы 2 – 7; в разделе 8 подразделы 80, 81, 82, 83, 85, 86, 87, 88; в разделе 9 подраздел 91). К изданиям, имеющим значительную историческую, художественную или иную культурную ценность для общества, до принятия экспертной комиссией Роскомнадзора (протокол от 16.01.2013 г.) критериев отнесения произведений художественной литературы к данной категории, к изданиям, имеющим значительную историческую, художественную или иную культурную ценность для общества, следует относить произведения древнерусской литературы, литературы древнего мира (литература Древнего Востока, античная литература), а также произведения российских и зарубежных авторов до первой четверти ХХ века, получивших общественное признание, всемирную известность; авторов, признанных (временем и специалистами) выразителями сущности определённых направлений в искусстве, литературных течений, создателей канонических произведений в рамках жанра и т.п.

1.4. Прочая информационная продукция (печатная) относимая к разделу ББК 84, поступившая в фонды библиотеки без знака информационной продукции подлежит обязательной классификации и маркировке.

2. Порядок классификации документов из библиотечного фонда

2.1. Классификация информационной продукции осуществляется в соответствии с требованиями Закона №436-ФЗ по следующим категориям информационной продукции с последующей маркировкой знаками информационной продукции:

- информационная продукция для детей, не достигших возраста шести лет – «0+»;

- информационная продукция для детей, достигших возраста шести лет – «6+»;

- информационная продукция для детей, достигших возраста двенадцати лет – «12+»;

- информационная продукция для детей, достигших возраста шестнадцати лет – «16+»;

- информационная продукция, запрещённая для детей (информационная продукция, содержащая информацию, предусмотренную частью 2 статьи 5 Федерального закона № 436-ФЗ) – «18+».

2.2. Классификация и маркировка информационной продукции, поступившей в фонды библиотеки после 1 сентября 2012 года без знака информационной продукции, осуществляется Комиссией по возрастной классификации информационной продукции библиотечно-информационного центра (далее - Комиссия).

2.3. При осуществлении классификации информационной продукции оценивается:

- тематика, жанр, содержание и художественное оформление;

- особенности восприятия содержащейся информации детьми определённой возрастной категории;

- вероятность причинения содержащейся в ней информацией вреда здоровью и (или) развитию детей.

2.4. Критерии классификации информационной продукции:

0+ Информационная продукция, содержащая информацию, не причиняющую вреда здоровью и (или) развитию детей (в том числе информационная продукция, содержащая оправданные ее жанром и (или) сюжетом эпизодические ненатуралистические изображение или описание физического и (или) психического насилия (за исключением сексуального насилия) при условии торжества добра над злом и выражения сострадания к жертве насилия и (или) осуждения насилия).

6+Информационная продукция

0+, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) кратковременные и ненатуралистические изображение или описание заболеваний человека (за исключением тяжелых заболеваний) и (или) их последствий в форме, не унижающей человеческого достоинства;

2) ненатуралистические изображение или описание несчастного случая, аварии, катастрофы либо ненасильственной смерти без демонстрации их последствий, которые могут вызывать у детей страх, ужас или панику;

3) не побуждающие к совершению антиобщественных действий и (или) преступлений эпизодические изображение или описание этих действий и (или) преступлений при условии, что не обосновывается и не оправдывается их допустимость и выражается отрицательное, осуждающее отношение к лицам, их совершающим.

12+ Информационная продукция

6+, а также информационная продукция, содержащая оправданные её жанром и (или) сюжетом:

1) эпизодические изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

2) изображение или описание, не побуждающие к совершению антиобщественных действий (в том числе к потреблению алкогольной и спиртосодержащей продукции, пива и напитков, изготавливаемых на его основе, участию в азартных играх, занятию бродяжничеством или попрошайничеством), эпизодическое упоминание (без демонстрации) наркотических средств, психотропных и (или) одурманивающих веществ, табачных изделий при условии, что не обосновывается и не оправдывается допустимость антиобщественных действий, выражается отрицательное, осуждающее отношение к ним и содержится указание на опасность потребления указанных продукции, средств, веществ, изделий;

3) не эксплуатирующие интереса к сексу и не носящие возбуждающего или оскорбительного характера эпизодические ненатуралистические изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

16+ Информационная продукция

12+, а также информационная продукция, содержащая оправданные ее жанром и (или) сюжетом:

1) изображение или описание несчастного случая, аварии, катастрофы, заболевания, смерти без натуралистического показа их последствий, которые могут вызывать у детей страх, ужас или панику;

2) изображение или описание жестокости и (или) насилия (за исключением сексуального насилия) без натуралистического показа процесса лишения жизни или нанесения увечий при условии, что выражается сострадание к жертве и (или) отрицательное, осуждающее отношение к жестокости, насилию (за исключением насилия, применяемого в случаях защиты прав граждан и охраняемых законом интересов общества или государства);

3) информация о наркотических средствах или о психотропных и (или) об одурманивающих веществах (без их демонстрации), об опасных последствиях их потребления с демонстрацией таких случаев при условии, что выражается отрицательное или осуждающее отношение к потреблению таких средств или веществ и содержится указание на опасность их потребления;

4) отдельные бранные слова и (или) выражения, не относящиеся к нецензурной

брани;

5) не эксплуатирующие интереса к сексу и не носящие оскорбительного характера изображение или описание половых отношений между мужчиной и женщиной, за исключением изображения или описания действий сексуального характера.

18+ К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера.

2.5. Решение о присвоении знака информационной продукции, принятое Комиссией оформляется протоколом. Протоколы хранятся в документах библиотеки в течение 5 лет, после чего в установленном порядке сдаются в архив.

2.6. Решение является основанием для размещения знака информационной продукции на той информационной продукции, оборот которой без знака запрещён, а также для размещения знака информационной продукции при создании машиночитаемой библиографической записи и печатной карточки. Обязанность по маркировке возложена на педагога- библиотекаря и педагога- организатора.

2.6.1. В отношении информационной продукции, запрещённой для детей, знак информационной продукции в обязательном порядке размещается на первой стороне обложки издания. Знак информационной продукции по размеру не должен быть меньше шрифтов, используемых на обложке.

2.6.2. Знак информационной продукции об ограничении распространения данной информационной продукции среди детей указывается на полосе издания, содержащей выходные сведения.

2.6.3. Электронные версии печатного издания, аудиокниги маркируются знаком информационной продукции, идентичным знаку, указанному печатной версии издания.

3. Порядок классификации информационной продукции, демонстрируемой во время проведения публичных мероприятий

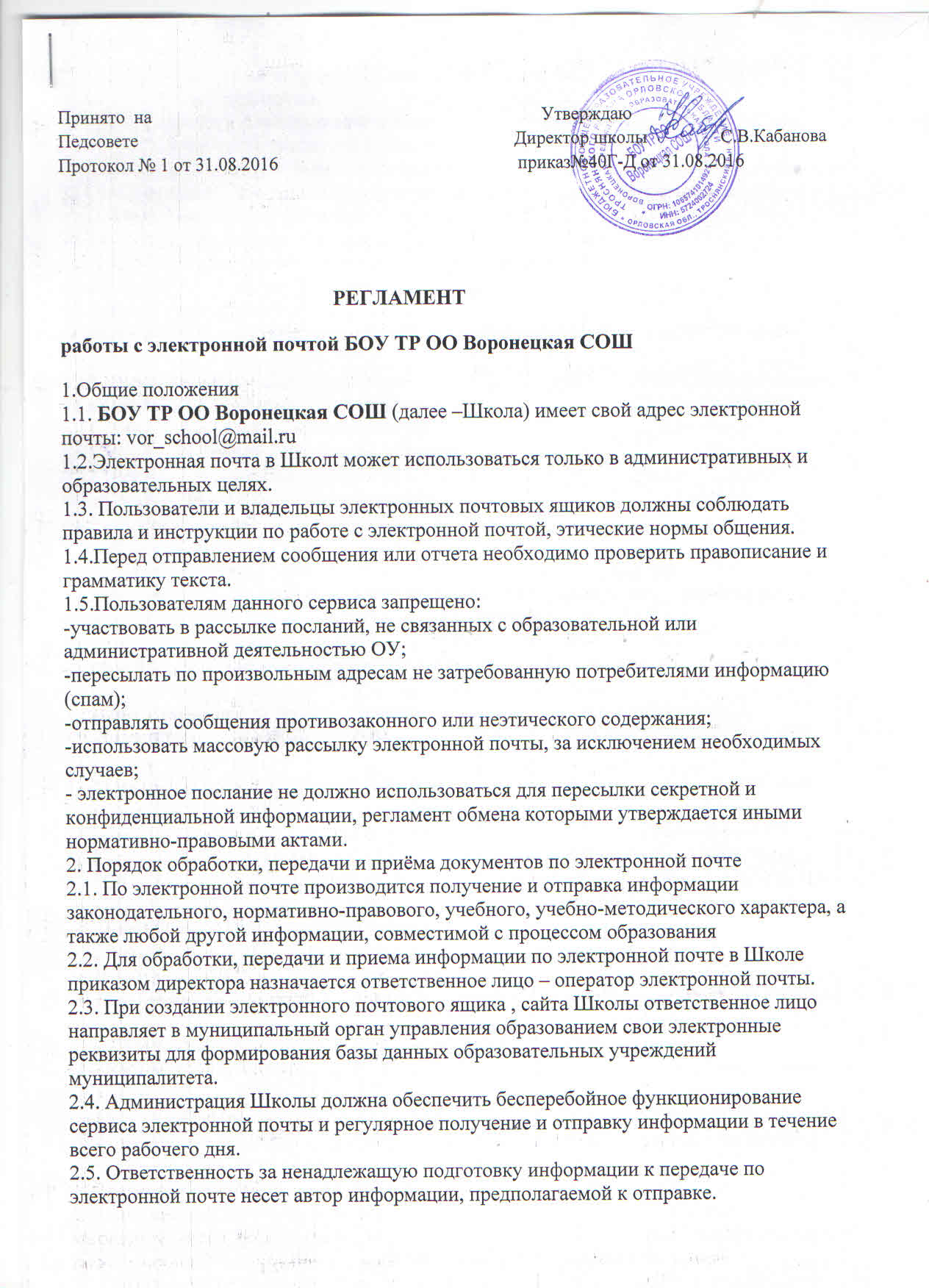
3.1. Вся информация, используемая во время проведения публичных мероприятий, подлежит классификации. К информационной продукции, используемой во время проведения публичного мероприятия относятся: издательская продукция, распространяемая среди читателей, презентационные и видео

3.4. Знак информационной продукции проставляется на рекламном объявлении, программе мероприятий.

3.5. В случае если в рекламном объявлении даётся информация о цикле мероприятий, предназначенных для различных возрастных групп, знак информационной продукции проставляется напротив названия каждого мероприятия.

3.6. Знак информационной продукции размещается на афишах и иных объявлениях о проведении мероприятия, а также на входных билетах, приглашениях и иных документах, предоставляющих право его посещения. На афишах и объявлениях знак информационной продукции размещается в правом нижнем углу. Размер знака информационной продукции должен составлять не менее чем 5 % площади объявления о проведении соответствующего зрелищного мероприятия.

3.7. Демонстрация посредством мероприятия информационной продукции, осуществляется непосредственно перед началом мероприятия звуковым сообщением о недопустимости или об ограничении присутствия на такой демонстрации детей соответствующих возрастных категорий.



2.6. Ответственность за отправку адресату и получение электронной почты несет оператор электронной почты.

2.7. Передаваемые с помощью электронной почты официальные документы должны иметь исходящий регистрационный номер.

2.8. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом. Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями по делопроизводству, утвержденными в Школе.

2.9. При получении электронного сообщения оператор:

-передает документ на рассмотрение администрации Школы или в случае именного сообщения - непосредственно адресату;

-в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.

2.10. Отправка и получение электронных документов осуществляется с использованием программных продуктов, предназначенных для работы с электронной почтой в Школе.

2.11. Учет электронных документов осуществляется путем регистрации в журнале регистрации входящих / исходящих документов.

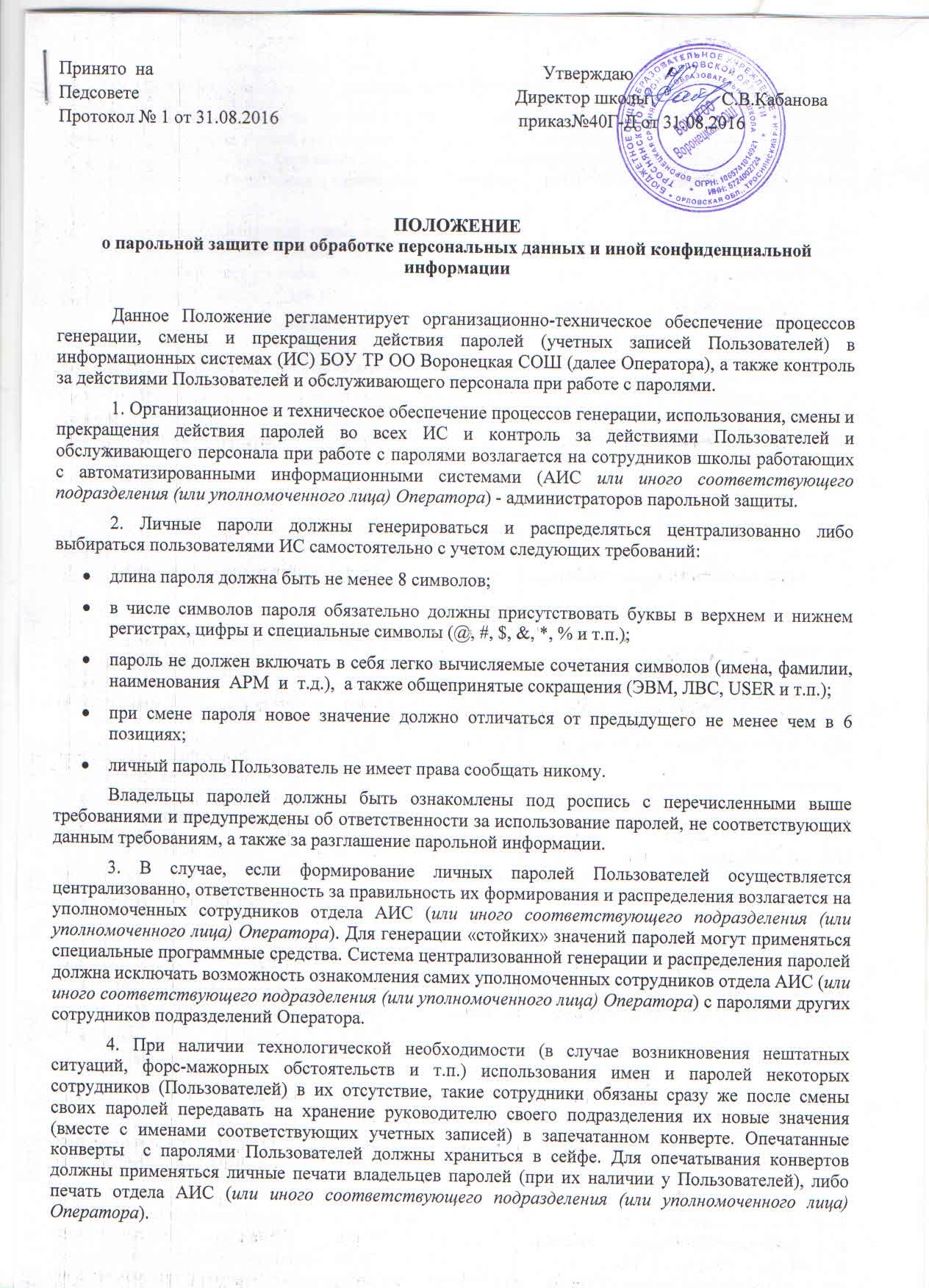
2.12. Электронные документы дублируются в виде копий на бумажных носителях с присвоением номера входящего или исходящего документа. Сроки их хранения регламентируются иными нормативными актами.

3. Ответственность

3.1. Изменение наименования официального эл. почтового адреса Школы согласовывает со специалистами отдела образования, ведущими электронный документооборот и отвечающими за информатизацию системы муниципального образования.

3.2. По факту изменения официального адреса эл. почты Школа обязана уведомить информационным письмом отдел образования за 3 рабочих дня до смены адреса эл. почты с указанием даты, с которой изменения вступают в силу.

3.3. Ответственность за функционирование электронного документооборота в учреждении несет директор Школы.



5. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал *(или в иные установленные Оператором сроки)*.

6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) немедленно после окончания последнего сеанса работы данного Пользователя с системой.

7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 6 или п. 7 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном личной печатью конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).

10. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль – возлагается на сотрудников отдела АИС (*или иного соответствующего подразделения (или уполномоченного лица) Оператора*) – администраторов парольной защиты.