

Приложение № 2

к приказу СПб ГБУСО «ДДИ № 1» от
01.10.2019 № 157-A-01

Санкт-Петербургское государственное бюджетное стационарное учреждение социального обслуживания «Дом-интернат для детей-инвалидов и инвалидов с детства с нарушениями умственного развития № 1»



УТВЕРЖДАЮ

Директор

СПб ГБУСО «ДДИ № 1»

В.Н. Асикритов

1 » октября 2019 г.

ПОЛОЖЕНИЕ

**об обработке и защите персональных данных
сторонних субъектов персональных данных в
Санкт-Петербургском государственном бюджетном
стационарном учреждении социального обслуживания
«Дом-интернат для детей-инвалидов и инвалидов с детства с
нарушениями умственного развития № 1»**

СОГЛАСОВАНО

Заместитель директора по общим вопросам

С.Н. Леонов

Начальник отдела кадров

Н.И. Алейникова

Юрисконсульт

О.В. Быстрова

г. Санкт-Петербург

20__ г.

Оглавление

1. Общие положения	
2. Принципы обработки персональных данных	
3. Сбор, обработка и хранение персональных данных	
4. Доступ к персональным данным	
5. Права субъекта персональных данных	
6. Обязанности оператора персональных данных	
7. Безопасность и защита персональных данных	
8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных	
Приложение №1 . Перечень нормативно-правовых актов по защите персональных данных ..	

1. Общие положения

1.1. Настоящее Положение об обработке и защите персональных данных сторонних субъектов персональных данных (далее – Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 N 152-ФЗ «О персональных данных», иными нормативно-правовыми актами, действующими на территории Российской Федерации (перечень нормативно-правовых актов указан в Приложении) и применяется в Санкт-Петербургском государственном бюджетном стационарном учреждении социального обслуживания «Дом-интернат для детей-инвалидов и инвалидов с детства с нарушениями умственного развития № 1» (далее – Учреждение).

1.2. Положение устанавливает порядок сбора, хранения, обработки и защиты персональных данных сторонних субъектов персональных данных (лиц, не являющихся работниками Учреждения).

1.3. Положение предназначено для работников Учреждения, имеющих доступ к персональным данным сторонних субъектов персональных данных (далее – персональные данные).

1.4. В настоящем Положении используются следующие понятия:

1) **персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая для выполнения основных видов деятельности Учреждения;

2) **специальные категории персональных данных** – информация, касающаяся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

3) **биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность;

4) **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;

5) **оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

6) **конфиденциальность персональных данных** – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или иного законного основания;

7) **целостность персональных данных** – состояние персональных данных, при котором отсутствует любое их изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

8) **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

9) **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

10) **использование персональных данных** – действия (операции) с персональными данными, совершаемые работником Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов

персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

11) **блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

12) **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;

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

14) **общедоступные персональные данные** – персональные данные, доступ к которым неограниченного круга лиц предоставлен с согласия субъекта персональных данных или на которые в соответствии с Федеральными законами не распространяется требование соблюдения конфиденциальности;

15) **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

16) **информация** – сведения (сообщения, данные) независимо от формы их представления;

17) **документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;

18) **носитель информации (материальный носитель)** – любой материальный объект бумажный и электронный, способный достаточно длительное время сохранять (нести) в своей структуре занесённую в/на него информацию.

1.5. Все работники Учреждения, допущенные до обработки персональных данных сторонних субъектов персональных данных, должны быть ознакомлены с настоящим Положением под роспись.

2. Принципы обработки персональных данных

2.1. Обработка персональных данных должна осуществляться на основе принципов:

- 1) законности целей и способов обработки персональных данных;
- 2) соответствия целей обработки персональных данных заранее определенным и заявленным целям при сборе персональных данных;
- 3) соответствия объема и содержания обрабатываемых персональных данных заявленным целям обработки персональных данных;
- 4) достоверности и актуальности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- 5) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2.2. Учреждение осуществляет обработку персональных данных различными способами. Обработка осуществляется с использованием средств автоматизации и без использования таких средств.

2.3. Учреждение не принимает 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 случая, когда такое решение принимается 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. Сбор, обработка и хранение персональных данных

3.1. Для осуществления основных видов деятельности в Учреждении происходит сбор персональных данных непосредственно с субъектов персональных данных и получение персональных данных субъектов от организаций, непосредственно собирающих персональные данные с субъектов.

3.2. При сборе персональных данных непосредственно с субъекта персональных данных необходимо получить его письменное согласие на обработку. Письменное согласие субъекта ПДн на обработку персональных данных должно включать в себя:

- 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) наименование и адрес Учреждения, получающего согласие субъекта ПДн;
- 3) цель обработки персональных данных;
- 4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- 5) перечень третьих лиц, кому работники Учреждения могут передавать эти персональные данные;
- 6) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- 7) срок, в течение которого действует согласие, а также порядок его отзыва.

3.3. При получении персональных данных от сторонних организаций, непосредственно собирающих персональные данные с субъекта, необходимо 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 Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» права субъекта персональных данных;
- 5) источник получения персональных данных.

3.4. Учреждение освобождается от обязанности предоставить субъекту персональных данных сведения, перечисленные в предыдущем пункте, в случаях, если:

- 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных работниками Учреждения;
- 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) работники Учреждения осуществляют 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 в предыдущем пункте, нарушает права и законные интересы третьих лиц.

3.5. Учреждение вправе проводить обработку персональных данных без согласия субъекта персональных данных при наличии одного из следующих оснований:

1) 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;

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

3) 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;

4) 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;

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

6) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) 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;

8) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, при условии обязательного обезличивания персональных данных;

9) 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);

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

3.6. Учреждение вправе обрабатывать специальные категории персональных данных в следующих случаях:

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

2) персональные данные сделаны общедоступными субъектом персональных данных;

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

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

5) обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

6) 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;

7) 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;

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

9) 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-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

10) 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.

3.7. Учреждение вправе обрабатывать биометрические персональные данные в следующих случаях:

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

2) обработка персональных данных осуществляется в связи с реализацией международных договоров Российской Федерации о реадмиссии;

3) обработка персональных данных осуществляется в связи с осуществлением правосудия и исполнением судебных актов;

обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию.

3.8. Передача персональных данных сторонним организациям осуществляется с согласия субъекта ПДн за исключением оснований, указанных в пункте 3.5 настоящего Положения.

3.9. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении, если срок хранения не установлен Федеральным законом или договором.

4. Доступ к персональным данным

4.1. Доступ к персональным данным субъектов ПДн имеют работники Учреждения согласно своим должностным обязанностям.

5. Права субъекта персональных данных

5.1. 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 Учреждением 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 Федеральными законами.

6. Обязанности оператора персональных данных

6.1. Работники Учреждения, 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.

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

6.3. 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.

6.4. 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.

6.5. 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.

6.6. 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.

6.7. 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.

6.8. 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.

6.9. В случае отсутствия возможности уничтожения персональных данных в течение установленного срока, 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.

7. Безопасность и защита персональных данных

7.1. При обработке персональных данных необходимо принимать организационно-правовые и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

7.2. Защита персональных данных субъекта от их неправомерного использования (несанкционированного доступа) или утраты ПДн обеспечивается Учреждением за счет его средств в порядке, установленном Федеральным законом и другими нормативными актами в области защиты персональных данных.

7.3. Материальные носители персональных данных (бумажные и электронные) маркируются и учитываются в специальных журналах Учреждения.

7.4. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Материальные носители с персональными данными должны храниться в запирающихся на ключ помещениях, металлических шкафах, сейфах, иных шкафах, имеющих запираемые блок-секции.

7.5. Персональные данные в электронном виде должны обрабатываться и храниться в защищенных, согласно Федеральному закону и другим нормативным актами в области защиты персональных данных, информационных системах Учреждения.

7.6. В каждом отделе Учреждения, обрабатывающем персональные данные, должен быть назначен ответственный работник.

7.7. После достижения цели обработки персональных данных они должны быть уничтожены установленным порядком.

7.8. Передача носителей с персональными данными возможна только курьерской доставкой или заказным письмом с описью вложения.

7.9. Передача персональных данных по открытым телекоммуникационным сетям общего пользования возможна только при использовании сертифицированных Федеральной службой безопасности Российской Федерации средств шифрования.

7.10. Необходимо рациональным образом размещать рабочие места работников, при котором исключалось бы бесконтрольное использование защищаемой информации, а также визуальный доступ к мониторам компьютеров, на которых обрабатываются персональные данные.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными Федеральными законами, а также несут гражданско-правовую и административную ответственность предусмотренную законодательством Российской Федерации.

Юрисконсульт отделения социальной помощи



С.В. Баланчивадзе

Приложение
к Положению об обработке и защите персональных данных
сторонних субъектов персональных данных
в СПб ГБУСО «ДДИ №1»

**Перечень нормативно-правовых актов по защите персональных
данных**

**Перечень основных действующих документов
в области защиты информации
(по состоянию на 13.08.2014)**

Подготовлен отделом информационно-компьютерной безопасности КИС

**I Перечень основных действующих документов в области технической
защиты информации**

Федеральные Законы	
1.	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями от 05.05.2014 № 97-ФЗ)
2.	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями от 04.06.2014 № 142-ФЗ)
3.	Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями от 28.06.2014 № 184-ФЗ)
4.	Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» (в редакции от 23.06.2014 № 160-ФЗ)
5.	Закон Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности»
6.	Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» (редакция, действующая от 21.12.2013 № 377-ФЗ)
7.	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с изменениями от 11.07.2011 № 200-ФЗ)
8.	Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (с изменениями от 21.07.2014 № 228-ФЗ)
9.	Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями от 02.07.2013 № 185-ФЗ)
10.	Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (выписка в части вопросов защиты информации) (с изменениями от 21.07.2014 № 277-ФЗ)
11.	Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (выписка в части вопросов защиты информации) (с изменениями и дополнениями от 21.07.2014 № 277-ФЗ)
12.	Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (глава 14) (с изменениями от 28.06.2014 № 199-ФЗ)
Указы Президента Российской Федерации	
1.	Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (с изменениями от 25.07.2014 № 529)
2.	Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 23.09.2005 № 1111)
3.	Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (в ред. Указа Президента РФ от 21.12.2013 № 940)
4.	«Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895
5.	Указ Президента Российской Федерации от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»

6.	Указ Президента Российской Федерации от 25.07.2013 № 648 «О формировании системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия»
7.	Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.

	Постановления Правительства Российской Федерации
1.	Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденное постановлением Совета Министров - Правительства Российской Федерации от 15.09.1993 № 912-51
2.	Постановление Правительства РФ от 15.05.2010 № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в заграничных учреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации»
3.	Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»)
4.	Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»)
5.	Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
6.	Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
7.	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
8.	Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
9.	Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» (в ред. от 20.07.2012 № 740)
10.	Постановление Правительства Российской Федерации от 14.09.2012 № 928 (в ред. от 21.07.2014 № 680) «О базовых государственных информационных ресурсах» (вместе с «Требованиями к порядку формирования, актуализации и использования базовых государственных информационных ресурсов», «Правилами формирования, актуализации и использования реестра базовых государственных информационных ресурсов»)

11.	Постановление Правительства Российской Федерации от 16.07.2012 № 722 «Правила предоставления документов по вопросам лицензирования в форме электронных документов»
Руководящие документы, нормативно-методические и методические документы	
1.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»)
2.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязи РФ) от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»
3.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязи РФ) от 21.12.2011 № 346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных»
4.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 19.08.2011 № 706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных»
5.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 15.03.2013 № 274 «Об утверждении перечня 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»
6.	«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 № 149/6/6-622)
7.	Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) «О вопросах отнесения фото- и видео - изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки»
8.	Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»
9.	Приказ Федеральной службы охраны Российской Федерации (ФСО РФ) от 07.08.2009 № 487 «Об утверждении Положения о сегменте информационно-телекоммуникационной сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации»

<u>Руководящие документы ФСТЭК России (Гостехкомиссии России)</u>	
<u>Нормативно-методические и методические документы</u>	
1.	Сборник руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России. М., 1998 г. В составе: Руководящий документ. Защита от несанкционированного доступа к информации Термины и определения. Гостехкомиссия России, 1992 г. Руководящий документ. Концепция защиты средств вычислительной техники автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992 г. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992 г. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992 г. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах средств вычислительной техники. Гостехкомиссия России, 1992 г. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1997 г. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Гостехкомиссия России, 1997 г. Руководящий документ. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Гостехкомиссия России, 1998 г.
2.	Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992 г.
3.	Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 04.06.1999 № 114.
4.	Руководящий документ Гостехкомиссии России «Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам» Гостехкомиссия России, 1999 г.
5.	Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом председателя Гостехкомиссии России от 19.06.2002 № 187.

6.	Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25.11.1994
7.	«Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», Гостехкомиссия России, 2002 г.
8.	«Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, 2002 г.
9.	«Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, 2002 г.
10.	«Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, 2002 г.
11.	Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации; Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (в учреждении, организации, утверждено Решением Гостехкомиссии России от 14.03.1995 № 32
12.	Типовые требования к содержанию и порядку разработки руководств по защите информации на объектах, утверждены Решением Гостехкомиссии России от 03.10.1995 № 42
13.	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом председателя Гостехкомиссии России от 30.08.2002 № 282 Извещение № 1 – 2008 о корректировке СТР-К.
14.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены Заместителем директора ФСТЭК России 15.02.2008
15.	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Заместителем директора ФСТЭК России 14.02.2008
16.	Решение ФСТЭК России, утвержденное первым заместителем директора ФСТЭК России от 05.03.2010
17.	Приказ ФСТЭК России от 18.02.2013 № 21 Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

18.	Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
19.	Методический документ «Меры защиты информации в государственных информационных системах» утвержден ФСТЭК России 11.02.2014
20.	Методические документы. Утверждены ФСТЭК России 14.06.2012 «Профили защиты средств антивирусной защиты»
21.	Методические документы. Утверждены ФСТЭК России 06.03.2012 «Профили защиты систем обнаружения вторжений»
22.	Методические документы. Утверждены ФСТЭК России 03.02.2012 «Профили защиты систем обнаружения вторжений»
23.	Руководящий документ. «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности» Гостехкомиссия России, 2003 г.
24.	Руководящий документ «Безопасность информационных технологий. Руководство по регистрации профилей защиты». Гостехкомиссия России, 2003 г.
25.	Руководящий документ. «Безопасность информационных технологий. Руководство по формированию семейств профилей защиты» Гостехкомиссия России, 2003 г.
26.	Руководящий документ. «Руководство по разработке профилей защиты и заданий по безопасности» Гостехкомиссия России, 2003 г.
27.	Информационное сообщение ФСТЭК России от 20.11.2012 № 240/22/4669 Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных
28.	Информационное письмо ФСТЭК России от 01.03.2012 № 240 «Об утверждении требований к системам обнаружения вторжений».
29.	Информационное сообщение ФСТЭК России от 30.07.2012 № 240/24/3095 Об утверждении требований в средствах антивирусной защиты
30.	Информационное сообщение ФСТЭК России от 04.05.2012 № 240/24/1701 О работах в области оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа
31.	Информационное сообщение ФСТЭК России от 15.07.2013 № 240/22/2637 по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

32.	Информационное сообщение ФСТЭК России от 25.07.2014 № 240/22/2748 "По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14.03.2014 № 31 "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды"
33.	Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, (решение Гостехкомиссии России 2002 г.). Извещение № 1 – 2007 о корректировке Сборника временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам.
34.	Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 № 27дсп
35.	Методические рекомендации по технической защите информации, составляющей коммерческую тайну, утверждённые заместителем директора ФСТЭК России 25.12.2006
36.	Пособие по организации технической защиты информации, составляющей коммерческую тайну, утверждённое заместителем директора ФСТЭК России 25.12.2006
37.	Решение Гостехкомиссии России от 21.12.1997 № 61 «О защите информации при вхождении России в международную информационную систему Интернет»

	<u>Государственные стандарты в области защиты информации и смежные с ними (ГОСТы)</u>
1.	ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».
2.	ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
3.	ГОСТ Р 51583-2000. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». Документ ограниченного распространения.
4.	ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» Документ ограниченного распространения
5.	ГОСТ 12.1.050-86 «Методы измерения шума на рабочих местах».
6.	ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».
7.	ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия». (с изменениями №2, утв. Приказом Ростехрегулирования от 11.03.2005 № 49-ст.)
8.	ГОСТ 2.601-2013 «Единая система конструкторской документации. Эксплуатационные документы».

9.	ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
10.	ГОСТ 34.602-2013 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создании автоматизированных систем».
11.	ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».
12.	ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
13.	РД 50-682-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения».
14.	РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».
15.	РД 50-680-88 «Методические указания. Автоматизированные системы. Основные положения».
16.	ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания».
17.	ГОСТ 6.10.4-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения».
18.	ГОСТ 28195-89 «Оценка качества программных средств. Общие положения».
19.	ГОСТ Р ИСО /МЭК 9126- 93 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению».
20.	ГОСТ 2.111-2013 «Нормоконтроль».
21.	ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации».
22.	ГОСТ 13661-92 «Совместимость технических средств электромагнитная. Пассивные помехоподавляющие фильтры и элементы. Методы измерения вносимого затухания».
23.	ГОСТ 29216-91 «Совместимость технических средств электромагнитная. Радиопомехи промышленные от оборудования информационной техники. Нормы и методы испытаний».
24.	ГОСТ 22505-97 Совместимость технических средств электромагнитная. Радиопомехи промышленные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний
25.	ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний»

26.	ГОСТ Р 50948-2001. «Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности».
27.	ГОСТ Р 50949-2001 «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности».
28.	ГОСТ Р 50923-96 «Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения».
29.	ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»
30.	ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»
Нормативные правовые акты Санкт-Петербурга	
1.	Закон Санкт-Петербурга от 07.07.2009 № 371-70 «О государственных информационных системах Санкт-Петербурга» <u>(с изменениями от 29.11.2013 № 635-111)</u>
2.	Постановление Правительства Санкт-Петербурга от 30.12.2013 № 1095 «О системе закупок товаров, работ, услуг для обеспечения нужд Санкт-Петербурга» (в ред. от 09.07.2014 № <u>588</u>)
3.	Распоряжение Администрации Санкт-Петербурга от 08.08.2001 № 616-ра «О мерах, обеспечивающих отнесение сведений, содержащихся в государственных информационных ресурсах исполнительных органов государственной власти Санкт-Петербурга, к категории конфиденциальной информации» <u>(в редакции от 06.12.2001 № 1277-ра)</u>
4.	Распоряжение Администрации Санкт-Петербурга от 15.05.2002 № 751-ра «Об организации использования электронной цифровой подписи в электронных документах, хранимых, обрабатываемых и передаваемых в автоматизированных информационных и телекоммуникационных сетях и системах исполнительных органов государственной власти Санкт-Петербурга» (с изменениями от 07.10.2010 № 1359)
5.	Распоряжение Администрации Санкт-Петербурга от 06.12.2002 № 2532-ра «О создании Комиссии по защите информации в исполнительных органах государственной власти Санкт-Петербурга» (с изменениями от 22.06.2009 № 677)
6.	Распоряжение Администрации Санкт-Петербурга от 24.03.2003 № 525-ра «О совершенствовании обеспечения исполнительных органов государственной власти Санкт-Петербурга услугами телематических служб в защищенном варианте»
7.	Распоряжение Комитета по информатизации и связи Администрации Санкт-Петербурга от 24.04.2003 N 2-р "Об организации работы узла телематических служб исполнительных органов государственной власти Санкт-Петербурга"
8.	Распоряжение Администрации Санкт-Петербурга от 04.02.2003 № 220-ра «Об организации контроля за состоянием технической защиты информации ограниченного доступа в исполнительных органах государственной власти Санкт-Петербурга» (с изменениями от 03.08.2011 № 1095)
9.	Приказ Администрации Санкт-Петербурга от 19.02.2003 № 6-пв «О создании Комиссии по контролю за состоянием работ по технической защите информации ограниченного доступа в исполнительных органах государственной власти Санкт-Петербурга»

II Перечень основных действующих документов в области криптографической защиты информации

<u>Постановления Правительства Российской Федерации</u>	
1.	Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
<u>Руководящие документы ФСБ России</u>	
<u>Нормативно-методические и методические документы</u>	
1.	Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (в ред. Приказа ФСБ РФ от 12.04.2010 №173)
2.	Приказ ФСБ России от 11.04.2014 № 202 "Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по лицензированию деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны"
3.	Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден руководством 8 Центра ФСБ России 08.08.2009 № 149/7/2/6-1173

4.	Приказ ФСБ России от 30.08.2012 № 440 «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»
5.	Приказ ФСБ России от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»
6.	Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».
7.	Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра»
8.	Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144
9.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»)
10.	Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» утвержденные Руководителем Роскомнадзора 13.12.2013
11.	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

III Перечень основных действующих документов в области обеспечения безопасности общедоступной информации

<u>Федеральные Законы</u>	
1.	Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления (с изменениями от 28.12.2013 № 396-ФЗ)
<u>Постановления Правительства Российской Федерации</u>	
1.	Постановление Правительства Российской Федерации от 18.05.2009 № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».
<u>Руководящие документы, нормативно-методические и методические документы</u>	
1.	Приказ Министерства экономического развития Российской Федерации от 16.11.2009 № 470 «О требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти». (в ред. Приказа Минэкономразвития России от 14.12.2012 № 789)
2.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 25.08.2009 № 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»
3.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 27.06.2013 № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования»
4.	Приказ Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»
5.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 3.07.2013 № 155 «Об утверждении Методических указаний по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры»
<u>Нормативные правовые акты Санкт-Петербурга</u>	
1.	Закон Санкт-Петербурга от 16.07.2010 № 445-112 Об обеспечении доступа к информации о деятельности государственных органов Санкт-Петербурга(с изменениями от 27.12.2013 № 729-132)

2.	Постановление правительства Санкт-Петербурга от 29.06.2011 № 864 О мерах по реализации закона Санкт-Петербурга «Об обеспечении доступа к информации о деятельности государственных органов Санкт-Петербурга» (с изменениями от 04.07.2013 № 461)
----	--

IV Перечень основных действующих документов в области обеспечения безопасности ключевых систем информационной инфраструктуры (КСИИ)

Документы Совета безопасности Российской Федерации	
1.	Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации
2.	«Система признаков критически важных объектов и критериев отнесения, функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий» (утв. Секретарем Совета Безопасности Российской Федерации 08.11.2005).

Руководящие документы ФСТЭК России	
Нормативно-методические и методические документы	
1.	Приказ ФСТЭК России от 14.03.2014 №31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды"
2.	Информационное сообщение ФСТЭК России от 25.07.2014 №240/22/2748 "По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14.03.2014 № 31 "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды"
3.	Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 18.05.2007)
4.	Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 19.11.2007)
5.	Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена заместителем директора ФСТЭК России 18.05.2007)

6.	Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена заместителем директора ФСТЭК России 18.05.2007)
7.	Методические рекомендации по организации контроля состояния обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации (утверждены заместителем директора ФСТЭК России 18.11.2008 №246дсп)
8.	Положение о Реестре ключевых систем информационной инфраструктуры (утверждено приказом ФСТЭК России от 04.03.2009 №74)
9.	Методические рекомендации по формированию аналитического прогноза по комплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период (утверждено ФСТЭК России 23.04.2011)
10.	Приказ Минздравсоцразвития РФ от 22.04.2009 №205 "Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации"
<u>Государственные стандарты (ГОСТы)</u>	
1.	ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения»
2.	ГОСТ РО 0043-002-2012 «Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Система документов»