Приложение № 1

к письму

### ОБЗОР ФЕДЕРАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

### в области защиты информации

**Содержание**

**1. Организация защиты персональных данных**

1.1. Выполнение требований Федерального закона от 27.07.2016 № 152– ФЗ «О персональных данных»……………………………………………………….3

1.2. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687………………………………………………………………………..……16

1.3. Выполнение требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119…………………………………….…………………………18

1.4. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 18.02.2013 № 21…………………………………..………..18

**2. Организация защиты информации с использованием средств криптографической защиты информации……………………………...…..25**

2.1. Выполнение 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 утвержденной приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 …………….…25

2.2. Выполнение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 № 378……………………………………………………………………………..33

**3. Ответственность за нарушение требований законодательства в области защиты информации……………………………………..……..…43**

## **1. Организация защиты персональных данных**

## **1.1. Выполнение требований Федерального закона от 27.07.2016 № 152 – ФЗ «О персональных данных» (далее – ФЗ № 152)**

## **1.1.1. Проверка данных, содержащихся в Реестре операторов, осуществляющих обработку персональных данных на предмет актуальности сведений**

| **№№** | **Требование статьи 22 ФЗ № 152** | **Исполнение требования** |
| --- | --- | --- |
| 1. | **Часть 1 статьи 22:**Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Управление Роскомнадзора по Кировской области) о своем намерении осуществлять обработку персональных данных | Юридическое лицо включено в реестр операторов, осуществляющих обработку персональных данных (<https://rkn.gov.ru/personal-data/register/>)  |
| 2. | **Часть 3 статьи 22:** Уведомление уполномоченного органа по защите прав субъектов персональных данных (Управление Роскомнадзора по Кировской области) о своем намерении осуществлять обработку персональных данных направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. **Уведомление должно содержать следующие сведения**: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 Федерального закона от 27.07.2006 № 152– ФЗ, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
8. 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;
9. Дата начала обработки персональных данных;
10. Срок или условие прекращения обработки персональных данных;
11. Сведения о наличии или об отсутствии трансграничной передачи персональных данных;
12. Сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;
13. Сведения об обеспечении безопасности персональных данных
 | Уведомление направлено в установленной форме, содержание уведомления соответствует установленным требованиям |
| 3. | **Часть 7 статьи 22:**В случае изменения сведений, указанных в части 3 статьи 22, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных (Управление Роскомнадзора по Кировской области) в течение **десяти рабочих дней** с даты возникновения таких изменений или с даты прекращения обработки персональных данных | Реестр операторов, осуществляющих обработку персональных данных, содержит актуальные сведения об юридическом лице.(Электронные формы заявлений размещены по адресу https://pd.rkn.gov.ru/operators-registry/notification/) |

## **1.1.2. Выполнение правовых мер по ФЗ № 152**

| **№****п/п** | **Ссылка на нормативный документ** | **Требование нормативного документа** | **Рекомендации****по возможной реализации требования** |
| --- | --- | --- | --- |
| 1 | ст.5 ФЗ № 152 | Принципы обработки персональных данных | Обработка соответствует принципам обработки ПДн, установленным ст.5 ФЗ № 152Основные принципы:1. Законность и справедливость.
2. Цели обработки должны быть заранее установлены (ч.2).
3. Разделение ПДн и баз по несовместимым целям (ч.3).
4. Объем данных должен соответствовать целям (ч.4,5,6).
5. Точность и актуальность ПДн (ч.6)
6. Соблюдение сроков обработки ПДн (ч.7).
 |
| 2 | ст. 6 ФЗ № 152 | Наличие условий обработки персональных данных | В организации имеются условия для обработки персональных данных, перечисленные в ст. 6 ФЗ № 152:- имеются основания (ч.1 – 13 случаев)- соблюдены условия поручения обработки персональных данных другим лицам (ч.3, 4,5)Необходимо учесть ситуации:- оператор поручает обработку другому лицу- другое лицо поручает обработку оператору- оператор и другое лицо передают друг другу ПДн (передача ПДн) |
| 3 | ст.7. ФЗ № 152 | 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 | Раскрытие персональных данных третьим лицам производится при наличии:1) Либо согласия субъекта персональных данных;2) Либо нормативно-правовых оснований, установленных федеральным законом |
| 4 | ст. 9ФЗ № 152 | Согласие субъекта персональных данных на обработку его персональных данных | Наличие согласия на обработку персональных данных (при отсутствии иных условий обработки, перечисленных в п. 2-11 части 1 ст. 6 ФЗ № 152).Согласие должно быть конкретным, информированным и сознательным.Согласие МОЖЕТ БЫТЬ ОТОЗВАНО. Поэтому, если оно берется, то Оператор должен предусматривать, что он будет делать в случае отзыва согласия.Согласия выполняются в двух формах:1. Согласие может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.
2. Согласие в письменной форме. Требования к письменной форме установлены частью 4 ст. 9 ФЗ № 152. Такое согласие необходимо НЕ ВСЕГДА, а только в отдельных случаях, предусмотренных Федеральными законами:

- обработка специальных категорий ПДн (ст. 10);- обработка биометрических персональных данных для идентификации субъекта ПДн (ст.11);- передача ПДн в страны, не обеспечивающие адекватную защиту персональных данных (ст.12); - принятие решений на основании исключительно автоматизированной обработки персональных данных (ст.16)- передача ПДн работников третьим лицам (ст. 88 ТК РФ)Во всех таких случаях имеются исключения, поэтому согласие в письменной форме требуется не всегда и нужно изучать ситуацию и соответствующую статью.**Важно!** Согласие в письменной форме оформляется **отдельное на каждую цель** обработки ПДн (до внесения изменений в 152-ФЗ данная норма действительна). Согласие в письменной форме может быть подписано электронной подписью и предоставлено в электронном виде. |
| 5 | ст. 10 ФЗ № 152 | Выполнение условий обработки специальных категорий персональных данных | Если ведется обработка специальных категорий персональных данных (касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни), то необходимо:– наличие письменного согласия субъекта персональных данных на обработку специальных категорий персональных данных;– документальное подтверждение причин обработки в соответствии со статьей 10 ФЗ № 152 |
| 6 | ст. 10.1 ФЗ № 152 | Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения | 1. Наличие согласия на обработку персональных данных, которые разрешены субъектом для распространения (за исключением случаев, когда обработка персональных данных осуществляется в целях выполнения возложенных законодательством полномочий и обязанностей. Указанное согласие **оформляется отдельно** от других согласий.2. Если сам субъект раскроет свои личные данные, но не предоставит согласие, обязанность доказать правомерность их распространения лежит на всех лицах, которые распространили эти сведения.3. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору:1) непосредственно;2) с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных (будет разработана до 01.07.2021).4. В согласии должно быть четко сформулировано, на что конкретно согласен субъект, условия и запретына обработку персональных данных, категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты.5. Оператор обязан опубликовать информацию об условиях обработки персональных данных, разрешенных субъектом к распространению и запретах, наложенных субъектом в течении 3 дней после получения согласия. |
| 7 | Ст.11 ФЗ № 152 | Биометрические персональные данные | В соответствии с ч.1.:- биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность - если они используются оператором для установления личности субъекта персональных данных, то их обработка для такой цели выполняется с согласия в письменной форме |
| 8 | Ст.14 ФЗ № 152 | Право субъекта персональных данных на доступ к его персональным данным | Субъект персональных данных имеет право на получение сведений, указанных в части 7 статьи 14, за исключением случаев, предусмотренных частью 8 статьи 14. 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.Сроки ответа на различные запросы приведены в разделе 1.1.4. обзора |
| 9 | Ст.16 ФЗ № 152 | Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных | 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, возможно при:1. Наличии согласия в письменной форме.
2. В случаях, определенных Законом.

К ситуациям, в которых производится принятие решения на основании исключительно автоматизированной обработки персональных данных, относятся, например автоматическая проверка выполненных заданий и выставление оценок. В законодательстве прописаны условия для работы системы государственной итоговой аттестации, использующей оценку результатов на основе сканирования и сверки в автоматическом режиме. Но, например, для онлайн-платформ обучения такие условия законодательство не устанавливает.  |
| 10 | Ст. 17 ФЗ № 152 | 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 |
| 11 | ст. 18 ФЗ № 152 | Обязанности оператора при сборе персональных данных | 1. Оператор должен разъяснять субъекту персональных данных юридических последствий отказа предоставить его персональные данные. Для этого должна быть утвержденная форма разъяснения. Рекомендуется для исполнителей разрабатывать типовые ответы для таких разъяснений.2. При сборе персональных данных запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации производится с использованием баз данных, находящихся на территории Российской Федерации. |

## **1.1.3. Выполнение организационных мер по ФЗ № 152**

|  |  |  |  |
| --- | --- | --- | --- |
| **№****п/п** | **Ссылка на нормативный документ** | **Требование нормативного документа** | **Рекомендации****по возможной реализации требования** |
| 1 | ст. 18.1ФЗ № 152 | Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом | Оператор обязан:1) назначить ответственного за организацию обработки персональных данных;2) издать документы: – определяющие политику оператора в отношении обработки персональных данных (опубликовать или иным образом обеспечить неограниченный доступ к документу, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно– телекоммуникационной сети), – локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;3) Применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 ФЗ № 1524) осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных законодательству и локальным актам оператора;4) провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер;5) проводить ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных и локальными актами по вопросам обработки персональных данных и (или) обучение указанных работников.6) 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 |
| 2 | ст. 19 ФЗ № 152 | Меры по обеспечению безопасности персональных данных при их обработке | 1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;5) учет машинных носителей персональных данных;6) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним (регламент резервного копирования);8) установление 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) проведение периодического контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных. |
| 3 | п. 4 ст. 21ФЗ № 152 | Соответствие сроков хранения персональных данных целям их обработки | 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 в срок, не превышающий **тридцати дней** с даты достижения цели обработки персональных данных |
| 4 | п. 3 ч. 4 ст. 22.1 ФЗ № 152 | Оператор назначает лицо, ответственное за организацию обработки персональных данных. | Лицо, ответственное за организацию обработки персональных данных 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. |

1.1.3. Сроки рассмотрения запросов субъектов персональных данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Статья 152-ФЗ, часть** | **Ситуация** | **Действие** | **Срок** | **Уведомление субъекта** |
| ст.20 ч.1 | Обращение субъекта или его представителя с требованием предоставить сведения, касающиеся обработки его ПДн согласно ст.14 ч.7 | Предоставление сведений, касающихся обработки ПДн субъекта (ст.14, ч.7) | При обращении или в срок до 30 календарных дней с момента обращения или получения запроса |  - |
| ст.20 ч.2 | Обращение субъекта или его представителя с требованием предоставить сведения, касающиеся обработки его ПДн | Мотивированный отказ с указанием положения, предусмотренного ч.8 ст.14. | При обращении или в срок до 30 календарных дней с момента обращения или получения запроса |  - |
| ст.20 ч.3 | Предоставление субъектом  сведений, подтверждающих неточность, неполноту или неактуальность ПДн | Внесение изменений в персональные данные (актуализация). | 7 рабочих дней с момента предоставления сведений | О внесенных изменениях |
| ст.20 ч.3 | Предоставление субъектом сведений, что данные получены незаконно или не соответствуют заявленным целям обработки | Уничтожение персональных данных | 7 рабочих дней с момента предоставления сведений | Об уничтожении (явно не указано) |
| ст.20 ч.4 | Обращение уполномоченного органа по защите прав субъектов ПДн (Роскомнадзор) | Предоставление Роскомнадзору необходимой информации | 30 календарных дней с даты получения запроса |  - |
| ст.21 ч.1 | Выявление неправомерной обработки (в результате обращения субъекта, его представителя или уполномоченного органа)  | блокирование неправомерно обрабатываемых ПДн или обеспечение блокирования (в случае обработчика) | с момента обращения или получения запроса (ст 14. ч.1) на период проверки |  - |
| ст.21 ч.1 | Выявление неточных ПДн (в результате обращение субъекта, его представителя или уполномоченного органа)  | блокирование неточных ПДн или обеспечение блокирования (в случае обработчика) | с момента обращения или получения запроса (ст 14. ч.1) на период проверки |  - |
| ст.21 ч.2 | Подтверждение факта неточных ПДн | уточнить данные (или обеспечить их уточнение) и снять блокирование | 7 рабочих дней со дня предоставления | О внесенных изменениях(ст.20 ч.3) |
| ст.21 ч.3 | Выявление факта неправомерной обработки ПДн | прекращение неправомерной обработки | 3 рабочих дня | Об устранении нарушений |
| ст.21 ч.3 | Невозможность обеспечения правомерности обработки | уничтожение персональных данных \* | 10 рабочих дней с даты выявления неправомерной обработки | Об уничтожении ПДн |
| ст.21 ч.4 | Достижение цели обработки ПДн | уничтожение персональных данных \* \*\* | 30 календарных дней с момента достижения цели |  - |
| ст.21. ч.5 | Отзыв субъектом согласия на обработку ПДн и если сохранение ПДн не требуется для целей обработки | Прекращение обработки и уничтожение ПДн \* \*\* | 30 календарных дней с даты поступления отзыва согласия |  - |

\* в случае отсутствия возможности уничтожения персональных данных в течение указанных сроков, 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.

\*\* 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 ФЗ "О персональных данных" или другими федеральными законами.

## **1.2. Выполнение требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687 (далее – требования Положения)**

| **№****п/п** | **Пункт****в требовании Положения** | **Требование нормативного документа** | **Рекомендации****по возможной реализации требования** |
| --- | --- | --- | --- |
| 1 | Пункт 4  | Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, обрабатываемой в организации | Фиксация персональных данных на отдельных материальных носителях персональных данных в специальных разделах или на полях форм (бланков) |
| 2 | Пункт 5 | При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. | Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель |
| 3 | Пункт 13  | Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ | Приказ об определении мест хранения персональных данных; Перечень лиц, осуществляющих обработку персональных данных. Документы по организации хранения, наличие и состояние сейфов, порядок закрытия и опечатывания сейфов.Соблюдение требований законодательства при обработке персональных данных работника кадровой службой (ст. 85 – ст. 90 Трудового кодекса Российской Федерации)В перечне мест хранения также рекомендуется установить сроки хранения документов. Сроки могут определяться исходя из анализа целей, сроков действия договоров, имеющихся оснований обработки персональных данных. Могут применяться в качестве основы для определения сроков:- Приказ Федерального архивного агентства от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения».- прямое указание в законодательстве на сроки обработки. |
| 4 | Пункт 14  | Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях | Организация раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях |
| 5 | Пункт 15  | При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором | Перечень лиц, имеющих доступ к местам хранения персональных данных (Проверка наличия охраны помещений, в которых ведется работа с персональными данными, документы по оборудованию помещений средствами защиты) |

## **1.3. Выполнение требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (далее – Требования к защите Персональных данных).**

| **№****п/п** | **Пункт в Требованиях к защите Персональных данных** | **Требование нормативного документа** | **Рекомендации по возможной реализации требования** |
| --- | --- | --- | --- |
|  | Пункты 7-12 | Определение типа угроз безопасности персональных данных, актуальных для информационной системы и уровня защищенности персональных данных | Акт определения уровня защищенности персональных данных |
|  | Пункты 13-16  | Выполнение пунктов Требований в зависимости от определенного уровня защищенности персональных данных (4,3,2,1 уровни) | Проведение организационных и технических мероприятий по реализации требований по определенному уровню защищенности |
|  | Пункт 17  | Контроль за выполнением требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом). | Организация проведения контроля в организации |

## **1.4. Выполнение требований Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 18.02.2013 № 21 (далее – приказ ФСТЭК № 21)**

| **№****п/п** | **Пункт в Приказе ФСТЭК № 21** | **Требование нормативного документа** | **Рекомендации по возможной реализации требования** |
| --- | --- | --- | --- |
| 1 | Пункт 4 приказа  | Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия. | Наличие документов на средства защиты, подтверждающих проведение оценки соответствия (сертификаты соответствия) |
| 2 | Пункт 8.1 приказа  | Реализация меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности). | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 3 | Пункт 8.2 приказа  | Реализация меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил. | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 4 | Пункт 8.3 приказа  | Реализация меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения. | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 5 | Пункт 8.4 приказа  | Реализация меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных. | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 6 | Пункт 8.5 приказа  | Реализация меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них. | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 7 | Пункт 8.6 приказа  | Реализация меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации. | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 8 | Пункт 8.7 приказа  | Реализация меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 9 | Пункт 8.8 приказа  | Реализация меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 10 | Пункт 8.9 приказа  | Реализация меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных. | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 11 | Пункт 8.10 приказа  | Реализация меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 12 | Пункт 8.11 приказа  | Реализация меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 13 | Пункт 8.12 приказа  | Реализация меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 14 | Пункт 8.13 приказа | Реализация меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно– телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 15 | Пункт 8.14 приказа  | Реализация меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |
| 16 | Пункт 8.15приказа  | Реализация меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений | Реализация данной меры обеспечивается в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационной системе, и на основании приложения к приказу ФСТЭК № 21 |

## **2. Организация защиты информации с использованием средств криптографической защиты информации**

## **2.1. Выполнение 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 утвержденной приказом Федерального агентства Правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 (далее – Инструкция ФАПСИ)**

| **№****п/п** | **Пункт в Инструкции ФАПСИ** | **Требование нормативного документа** | **Рекомендации по возможной реализации требования** |
| --- | --- | --- | --- |
| 1 | п.19 | Физические лица допускаются к работе с СКЗИ согласно **перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации**. До такого утверждения техническая возможность использования СКЗИ лицами, включенными в данный перечень, должна быть согласована с лицензиатом ФАПСИ. Лицензиаты ФАПСИ в рамках согласованных с обладателями конфиденциальной информации полномочий по доступу к конфиденциальной информации имеют право утверждать такой перечень в отношении подчиненных им должностных лиц. | Должен быть утвержден перечень пользователей СКЗИ |
| 2 | п.21 | Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения. | Возложение обязанностей на лицо, ответственное за СКЗИ по обучению пользователей и их допуску к работе с СКЗИНаличие журнала учета и допуска пользователей СКЗИ |
| 3 | п. 26  | Используемые или хранимые средства криптографической защиты информации (далее – СКЗИ), эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно– программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами. | Наличие журнала учета ключевых носителей;Наличие журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов |
| 4 | п. 27  | Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность | Журнал учета должен быть заполнен и содержать актуальные сведения |
| 5 | п.29 | Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована соответствующим органом криптографической защиты.Обладатель конфиденциальной информации с согласия органа криптографической защиты может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета. | Передача СКЗИ разрешается только внутри организации. Передавать СКЗИ между организации и лицам, не являющимся работниками организации не допускается. |
| 6 | п. 30  | Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей | Запираемые (а желательно и опечатываемые) ящики, шкафы, сейфы, в которых хранятся СКЗИ носители, эксплуатационная и техническая документация к СКЗИ, ключевые документы |
| 7 | П. 31 | Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно - программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища. | Опечатывание системного блока ПК, ноутбука. Варианты- саморазрушающиеся этикетки- устройство для опечатыввания- печать на бумаге, покрытая силикатным клеем |
| 8 | п.42. | Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования). | Применение носителей типа Rutoken с надежным стиранием, либо применение порядка уничтожения ключей, изложенного в правилах пользования СКЗИ. |
| 9 |  | Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах. | Необходимо соблюдать обязанность хранить сертификаты электронной подписи – ПОСТОЯННО. Они необходимы для подтверждения подлинности электронных документов в будущем.Проведение уничтожения секретных ключей и ключевых пар.Учет уничтожения:- разовое фиксируется в журнале учета лицом, ответственным за СКЗИ- уничтожение нескольких ключей, ключевых документов фиксируется по акту уничтожения  |
| 10 | П.47 | Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают в соответствующий орган криптографической защиты. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению лицензиата ФАПСИ, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной. | Регламентация процедуры реагирования на случаи компрометации (инциденты) в инструкции по эксплуатации СКЗИ. |
| 11 | п.48 | О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать в соответствующий орган криптографической защиты. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску. | Должно быть регламентировано в инструкции пользователю СКЗИ.Пользователям следует сообщать о таких случаях: * сотруднику, ответственному за СКЗИ;
* в удостовреяющий центр, выдавший сертификат электронной подписи;
* в организацию-лицензиат, отвечающую за обеспечение безопасности конкретной защищенной сети.
 |
| 12 | п.49 | Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации. | Должно быть регламентировано в инструкции по эксплуатации СКЗИ. |
| 13 | п. 51  | Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним (далее – спецпомещения), должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов | Специальные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.  |
| 14 | п. 62  | Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ | Реализация требования режимными мерами. |
| 15 | п. 63  | Режим охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации по согласованию с соответствующим органом криптографической защиты | Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции, специфику и условия работы конкретных пользователей СКЗИ.  |
| 16 | п. 64, п. 66  | В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ | У каждого пользователя должен быть свой (индивидуальный) опечатываемый шкаф. В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями. Ключи от хранилищ и помещений должны быть учтены в журнале учета.Должно быть назначено лицо, ответственное за учет, выдачу, замену, возврат ключей. |

## **2.2. Выполнение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 № 378 (далее – приказ ФСБ № 378).**

| **№****п/п** | **Пункты в приказе ФСБ № 378** | **Требование нормативного документа** | **Рекомендации по возможной реализации требования** |
| --- | --- | --- | --- |
| Для обеспечения 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований |
| 1 | Пункт 5  | Для обеспечения 4 уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение ряда требований | 1) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;2) обеспечение сохранности носителей персональных данных;3) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;4) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. |
| 2 | Пункт 6 | Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения | Достигается путем:1) оснащения Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;2) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;3) утверждения перечня лиц, имеющих право доступа в Помещения. |
| 3 | Пункт 7 | Обеспечение сохранности носителей персональных данных | 1) Осуществление хранения съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.2) Осуществление поэкземплярного учета машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров |
| 4 | Пункт 8  | Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей | Необходимо разработать и утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;Поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей |
| 5 | Пункт 9  | Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз | Использование для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше |
| Для обеспечения 3 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований для предыдущего уровня защищенности необходимо выполнение следующих требований |
| 1 | Пункты 16, 17 | Назначение должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе | Назначение обладающего достаточными навыками должностного лица (работника) оператора ответственным за обеспечение безопасности персональных данных в информационной системе |
| 2 | Пункт 18  | Использование СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2 типа.Использование СКЗИ класса КС1 и выше в случаях, когда для информационной системы актуальны угрозы 3 типа | Данная мера выполняется вместо данной в п. 4 таблицы |
| Для обеспечения 2 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований для предыдущего уровня защищенности необходимо выполнение следующих требований |
| 1 | Пункт 19  | Необходимо выполнение требования о том, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей | а) утверждение руководителем оператора списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии;б) обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений;в) обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений;г) обеспечение периодического контроля работоспособности указанных в [подпунктах "б"](#Par1) и ["в"](#Par2) настоящего пункта автоматизированных средств (не реже 1 раза в полгода) |
| 2 | Пункт 21  | Использование СКЗИ класса КА в случаях, когда для информационной системы актуальны угрозы 1 типа;Использование СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2 типа;Использование СКЗИ класса КС1 и выше в случаях, когда для информационной системы актуальны угрозы 3 типа | Данная мера выполняется вместо указанной в п. 4 настоящей таблицы |
| Для обеспечения 1 уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований для предыдущего уровня защищенности необходимо выполнение следующих требований |
| 1 | Пункт 22  | Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе | а) обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;б) отражение в электронном журнале безопасности полномочий сотрудников оператора персональных данных по доступу к персональным данным, содержащимся в информационной системе. Указанные полномочия должны соответствовать должностным обязанностям сотрудников оператора;в) назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия, отраженных в нем полномочий сотрудников оператора их должностным обязанностям (не реже 1 раза в месяц) |
| 2 | Пункт 22  | Создание отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение его функций на одно из существующих структурных подразделений | а) проведение анализа целесообразности создания отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе;б) создание отдельного структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение его функции на одно из существующих структурных подразделений |
| 3 | Пункт 25  | Дополнительные требования по организации режима обеспечения безопасности помещений, в которых размещена информационная система | а) оборудование окон Помещений, расположенные на первых и (или) последних этажах зданий, а также окон Помещений, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения;б) оборудование окон и дверей Помещений, в которых размещены серверы информационной системы, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения. |
| 4 | Пункт 25  | Использование СКЗИ класса КА в случаях, когда для информационной системы актуальны угрозы 1 типа;Использование СКЗИ класса КВ и выше в случаях, когда для информационной системы актуальны угрозы 2 типа | Данная мера выполняется вместо указанной в п. 4 таблицы |

## **Классы СКЗИ (пункты 10-14 приказа ФСБ № 378)**

В соответствии с уровнем защищенности персональных данных, обрабатываемых в информационных системах персональных данных, должен быть определен класс СКЗИ. В выборе класса СКЗИ важно опираться на Модель нарушителя и его возможности при реализации атак на информационную систему персональных данных.

СКЗИ определенного класса применяются для нейтрализации атак, при создании способов, подготовке и проведении которых используются возможности из числа перечисленных для предыдущего класса и не менее одной данного класса.

Классы СКЗИ и соответствующие возможности нарушителей представлены в таблице 1.

**Таблица 1 – Классы СКЗИ и соответствующие возможности нарушителей**

| **Класс СКЗИ** | **Возможности нарушителей** |
| --- | --- |
| КС1 | Создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ |
| Создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ |
| Проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее - контролируемая зона) |
| Проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:* внесение несанкционированных изменений в СКЗИ и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ и в совокупности представляющие среду функционирования СКЗИ (далее - СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ требований, в том числе с использованием вредоносных программ;
* внесение несанкционированных изменений в документацию на СКЗИ и компоненты СФ.
 |
| Проведение атак на этапе эксплуатации СКЗИ на:* персональные данные;
* ключевую, аутентифицирующую и парольную информацию СКЗИ;
* программные компоненты СКЗИ;
* аппаратные компоненты СКЗИ;
* программные компоненты СФ, включая программное обеспечение BIOS;
* аппаратные компоненты СФ;
* данные, передаваемые по каналам связи;
* иные объекты, которые установлены при формировании совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак с учетом применяемых в информационной системе информационных технологий, аппаратных средств (далее - АС) и программного обеспечения (далее - ПО).
 |
| Получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть "Интернет") информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация:* общие сведения об информационной системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы);
* сведения об информационных технологиях, базах данных, АС, ПО, используемых в информационной системе совместно с СКЗИ, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, АС, ПО, используемые в информационной системе совместно с СКЗИ;
* содержание конструкторской документации на СКЗИ;
* содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ и СФ;
* общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ;
* сведения о каналах связи, по которым передаются защищаемые СКЗИ персональные данные (далее - канал связи);
* все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного доступа к информации организационными и техническими мерами;
* сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, нарушениях правил эксплуатации СКЗИ и СФ;
* сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами, неисправностях и сбоях аппаратных компонентов СКЗИ и СФ;
* сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ и СФ.
 |
| Применение:* находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;
* специально разработанных АС и ПО.
 |
| Использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки:* каналов связи, не защищенных от несанкционированного доступа к информации организационными и техническими мерами;
* каналов распространения сигналов, сопровождающих функционирование СКЗИ и СФ.
 |
| Проведение на этапе эксплуатации атаки из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети. |
| Использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее - штатные средства). |
| КС2 | Проведение атаки при нахождении в пределах контролируемой зоны. |
| Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:* документацию на СКЗИ и компоненты СФ;
* помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.
 |
| Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:* сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;
* сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;
* сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.
 |
| Использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий. |
| КС3 | Физический доступ к СВТ, на которых реализованы СКЗИ и СФ. |
| Возможность располагать аппаратными компонентами СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий. |
| КВ | Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО. |
| Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий. |
| Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ. |
| КА | Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО. |
| Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ. |
| Возможность располагать всеми аппаратными компонентами СКЗИ и СФ. |

При выборе СКЗИ стоит обратить внимание на наличие сертификата соответствия требованиям ФСБ России и его актуальность. В процессе эксплуатации СКЗИ важно обеспечивать контроль использования СКЗИ и актуальности срока действия сертификата соответствия.

\_\_\_\_\_\_\_\_\_\_\_

**3. Ответственность за нарушение требований законодательства в области защиты информации**

Новые размеры штрафов действуют с 26.03.2021 после вступления в силу Федерального закона от 24.02.2021 № 19-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

|  |  |  |  |
| --- | --- | --- | --- |
| **№п.****ст.13.11** | **Краткое описание** | **Требование** | **Наказание** |
| 1 | Обработка персональных данных **в случаях, не предусмотренных законодательством РФ**, либо обработка персональных данных, **несовместимая с целями** сбора Персональных данных | Ст. 6 152-ФЗ | Предупреждение или штраф:Граждане: 2-6 т.р.Долж.лица:10-20 т.р.Юр.лица: 60-100 т.р. |
|  | **Повторное нарушение части 1** | Ст.6 152-ФЗ | Граждане: 4-12 т.р.Долж.лица:20-50 т.р.ИП: 50-100т.рЮр.лица: 100-300 т.р. |
| 2 | Обработка персональных данных **без согласия в письменной форме** или с нарушением письменной формы согласия | Ст. 9 152-ФЗ | Штраф- Граждане: 6-10 т.р.- Долж.лица:20-40 т.р.- Юр.лица: 30-150 т.р. |
|  | **Повторное нарушение части 2** | Ст. 9 152-ФЗ | Граждане: 10-20 т.р.Долж.лица:40-100 т.р.ИП: 100-300т.рЮр.лица: 300-500 т.р. |
| 3 | **Неопубликование политики обработки персональных данных** | Ст. 18.1 152-ФЗ | Предупреждение или штраф:- Граждане: 1,5-3 т.р.- Долж.лица:6-12 т.р.- ИП: 10-20 т.р.- Юр.лица: 30-60 т.р. |
| 4 | **Непредоставление субъекту персональных данных информации об обработке его персональных данных** | Ст. 14, ст.20 152-ФЗ | Предупреждение или штраф:- Граждане: 2-4 т.р.- Долж.лица:8-12 т.р.- ИП: 20-30 т.р.- Юр.лица: 40-80 т.р. |
| 5 | **Невыполнение требования субъекта персональных данных, его представителя, либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении** | Ст.21 152-ФЗ | Предупреждение или штраф:- Граждане: 2-4 т.р.- Долж.лица:8-20 т.р.- ИП: 20-40 т.р.- Юр.лица: 50-90 т.р. |
|  | **Повторное нарушение части 5** | Ст.21 152-ФЗ | Предупреждение или штраф:- Граждане: 20-30 т.р.- Долж.лица: 30-50 т.р.- ИП: 50-100 т.р.- Юр.лица: 300-500 т.р. |
| 6 | **Необеспечение сохранности персональных данных на материальных носителях** | Постановление Правительства Российской Федерации№ 687 | Штраф:- Граждане: 1,5-4 т.р.- Долж.лица:8-20 т.р.- ИП: 20-40 т.р.- Юр.лица: 50-100 т.р. |
| 7 | **Невыполнение государственным или муниципальным органом обязанности по обезличиванию персональных данных** | Постановление Правительства Российской Федерации № 211 | Предупреждение или штраф:- Долж.лица:6-12 т.р. |
| 13.12 | Нарушения правил защиты информации | 149-ФЗ,152-ФЗ,63-ФЗ | Штраф:- Долж.лица:1-2 т.р.- Юр.лица: 15-20 т.р. |
| 13.13 | Незаконная деятельность в области информационной безопасности | 99-ФЗ «О лицензировании отдельных видов деятельности» | Штраф- Долж.лица:2-3 т.р.- Юр.лица: 10-20 т.р. |
| 13.14 | Разглашение информации ограниченного доступа  | Информации, доступ к которой ограничен федеральным законом | Штраф:- Граждане: 0,5-1 т.р.- Долж.лица:4-5 т.р. |

\_\_\_\_\_\_\_\_\_\_\_