



СИСТЕМА УДАЛЕННОГО МОНИТОРИНГА  
И УПРАВЛЕНИЯ «АССИСТЕНТ»

**ПРАВОВЫЕ ОСНОВАНИЯ  
ИСПОЛЬЗОВАНИЯ  
СЕРТИФИЦИРОВАННЫХ СРЕДСТВ  
УДАЛЕННОГО ДОСТУПА**

ПО СОСТОЯНИЮ ЗАКОНОДАТЕЛЬСТВА НА 22 АВГУСТА 2022 ГОДА

Версия 4.0 от 29.08.2022 г.

Воронеж 2022

## Содержание

Введение .....	3
1. Государственные информационные системы .....	4
2. Информационные системы персональных данных .....	7
3. Автоматизированные системы управления производственными и технологическими процессами .....	10
4. Значимые объекты критической информационной инфраструктуры.....	11
5. Информационные системы финансовых организаций (банков).....	14
6. Информационные системы медицинских организаций.....	17
7. Сертификат соответствия ФСТЭК России № 4162 выдан 26.08.2019 .....	18
Заключение .....	19
Список использованных источников .....	20

## Введение

В случае принятия оператором решения о необходимости организации удаленного доступа (мониторинга и управления) к персональным компьютерам и/или серверам, входящим в состав информационных систем, относящихся к

- государственным информационным системам [1],
- информационным системам персональных данных [2],
- автоматизированным системам управления производственными и технологическими процессами [3],
- значимым объектам критической информационной инфраструктуры [4],
- информационным системам финансовых организаций (банков) [6];
- информационным системам медицинских организаций [7];

должны быть выполнены требования законодательства Российской Федерации к используемому прикладному программному обеспечению.

Ниже приведены правовые основания использования программного обеспечения, прошедшего процедуру оценки соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации (в системе сертификации ФСТЭК России) при организации удаленного доступа (мониторинга и управления).

## 1. Государственные информационные системы

Перечень и положения нормативно-правовых актов определяющих использование сертифицированных средств защиты информации для защиты информации в государственных информационных системах приведены в таблице 1.

Таблица 1.

Нормативный документ	Положения
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	<p><b>Статья 13. Информационные системы</b></p> <p><b>Подпункт 1 пункта 1</b> государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.</p> <p><b>Пункт 4.</b> Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.</p> <p><b>Пункт 5.</b> Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании таких информационных систем.</p>
	<p><b>Статья 14. Государственные информационные системы</b></p> <p><b>Пункт 8.</b> Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.</p>
	<p><b>Статья 16. Защита информации</b></p> <p><b>Пункт 5.</b> Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России – примечание</p>

Нормативный документ	Положения
	<p>ООО «САФИБ») и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России – примечание ООО «САФИБ»), в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.</p> <p><b>Пункт 6.</b> Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.</p>
<p>Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании»</p>	<p><b>Статья 4. Законодательство Российской Федерации о техническом регулировании</b></p> <p><b>Пункт 3.</b> Федеральные органы исполнительной власти вправе издавать в сфере технического регулирования акты только рекомендательного характера, за исключением случаев, установленных статьями 5 и 9.1 настоящего Федерального закона.</p> <p><b>Статья 5</b> касается, в том числе, и продукции, используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации к информации ограниченного доступа (в том числе служебная информация ограниченного распространения, имеющая пометку "Для служебного пользования" [5]).</p>
<p>Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»</p>	<p><b>Пункт 8.</b> В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.</p> <p><b>Пункт 11.</b> Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме</p>

Нормативный документ	Положения
	<p><i>обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ "О техническом регулировании"</i></p> <p><b>Пункт 20.</b> Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, ... должны обеспечивать: ... защиту информационной системы, ее средств, систем связи и передачи данных.</p> <p><b>Пункт 26.</b> В информационных системах 1 класса защищенности применяются сертифицированные средства защиты информации, <i>соответствующие 4 или более высокому уровню доверия.</i></p> <p>В информационных системах 2 класса защищенности применяются сертифицированные средства защиты информации, <i>соответствующие 5 или более высокому уровню доверия.</i></p> <p>В информационных системах 3 класса защищенности применяются сертифицированные средства защиты информации, <i>соответствующие 6 или более высокому уровню доверия.</i></p> <p>В информационных системах применяются средства защиты информации, <i>сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности).</i></p> <p><i>(Уровни доверия устанавливаются документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденным приказом ФСТЭК России от 02.06.2020 № 76 – примечание ООО «САФИБ»)</i></p>

## 2. Информационные системы персональных данных

Перечень и положения нормативно-правовых актов, определяющих использование сертифицированных средств защиты информации при обработке персональных данных в информационных системах персональных данных, приведены в таблице 2.

Таблица 2.

Нормативный документ	Положения
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	<p><b>Статья 16. Защита информации</b></p> <p><b>Пункт 2.</b> Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.</p> <p><b>Пункт 6.</b> Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.</p>
Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	<p><b>Статья 19. Меры по обеспечению безопасности персональных данных при их обработке</b></p> <p><b>Часть 1.</b> Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.</p> <p><b>Часть 2.</b> Обеспечение безопасности персональных данных достигается, в частности:...</p> <p>3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;...</p> <p><b>Часть 4.</b> Состав и содержание... требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных</p>

Нормативный документ	Положения
	<p>устанавливаются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (<i>ФСБ России – примечание ООО «САФИБ»</i>), и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (<i>ФСТЭК России – примечание ООО «САФИБ»</i>), в пределах их полномочий.</p>
<p>Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»</p>	<p><b>Пункт 4.</b> Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».</p> <p><b>Пункт 6.</b> ...Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.</p> <p><b>Пункт 13.</b> Для обеспечения 4-го уровня защищенности персональных данных (<i>минимальный уровень защищенности – примечание ООО «САФИБ»</i>) при их обработке в информационных системах необходимо выполнение следующих требований: ...г) <i>использование средств защиты информации, прошедших процедуру оценки соответствия</i> требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.</p>
<p>Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности</p>	<p><b>Пункт 4.</b> Меры по обеспечению безопасности персональных данных реализуются в том числе посредством <i>применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия</i>, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.</p> <p><b>Пункт 12.</b> Технические меры защиты персональных данных реализуются посредством применения средств защиты</p>



Нормативный документ	Положения
персональных данных при их обработке в информационных системах персональных данных»	<p>информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности...</p> <p>При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:</p> <p>в информационных системах 1 уровня защищенности персональных данных применяются <i>средства защиты информации не ниже 4 класса и 4 уровня доверия</i>, а также средства вычислительной техники не ниже 5 класса;</p> <p>в информационных системах 2 уровня защищенности персональных данных применяются <i>средства защиты информации не ниже 5 класса и 5 уровня доверия</i>, а также средства вычислительной техники не ниже 5 класса;</p> <p>в информационных системах 3 уровня защищенности персональных данных применяются <i>средства защиты информации 6 класса и 6 уровня доверия</i>, а также средства вычислительной техники не ниже 5 класса;</p> <p>в информационных системах 4 уровня защищенности персональных данных применяются <i>средства защиты информации 6 класса и 6 уровня доверия</i>, а также средства вычислительной техники не ниже 6 класса.</p> <p><i>(Уровни доверия устанавливаются документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденным приказом ФСТЭК России от 02.06.2020 № 76 – примечание ООО «САФИБ»)</i></p>

### 3. Автоматизированные системы управления производственными и технологическими процессами

Перечень и положения нормативно-правовых актов, определяющих использование сертифицированных средств защиты информации при обработке информации в автоматизированных системах управления производственными и технологическими процессами приведены в таблице 3.

Таблица 3.

Нормативный документ	Положения
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	<b>Статья 16. Защита информации</b> <b>Пункт 2.</b> Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.
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»	Пункт 24. ...В автоматизированных системах управления 1 и 2 классов защищенности <i>применяются сертифицированные средства защиты информации</i> , программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недеklarированных возможностей.  <i>Примечание ООО «САФИБ»:</i> <i>В соответствии с пунктом 19 документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденного приказом ФСТЭК России от 02.06.2020 № 76:</i> <i>19. К испытаниям по выявлению уязвимостей и недеklarированных возможностей средства предъявляются следующие требования:</i> <i>19.3. Испытания программного обеспечения средства, соответствующего 4 уровню доверия, должны быть проведены по 4 уровню контроля.</i>

#### 4. Значимые объекты критической информационной инфраструктуры

Перечень и положения нормативно-правовых актов, определяющих использование сертифицированных средств защиты информации и запрет на использование иностранного программного обеспечения при обработке информации в значимых объектах критической информационной инфраструктуры приведены в таблице 4.

Таблица 4.

Нормативный документ	Положения
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	<b>Статья 16. Защита информации</b> <b>Пункт 2.</b> Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.  <b>Пункт 6.</b> Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.
Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	<b>Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры</b> <b>Часть 1.</b> Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации ( <i>ФСТЭК России – примечание ООО «САФИБ»</i> ), дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры и этими требованиями предусматриваются:... <i>3) установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры.</i>  <b>Часть 2.</b> Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-

Нормативный документ	Положения
	<p>правовому регулированию в установленной сфере деятельности, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, могут устанавливать дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, содержащие особенности функционирования таких объектов в установленной сфере деятельности.</p>
<p>Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»</p>	<p><b>Пункт 28.</b> Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности <i>в формах обязательной сертификации</i>, испытаний или приемки.</p> <p><b>Пункт 29.</b> ... При этом в значимых объектах 1 категории значимости применяются <i>сертифицированные средства защиты информации</i>, соответствующие 4 или более высокому уровню доверия. В значимых объектах 2 категории значимости применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В значимых объектах 3 категории значимости применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.</p> <p><i>(Уровни доверия устанавливаются документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденным приказом ФСТЭК России от 02.06.2020 № 76 – примечание ООО «САФИБ»)</i></p>
<p>Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической</p>	<p><b>Пункт 1.</b>  <b>а)</b> с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (далее - <i>заказчики</i>), <i>не могут осуществлять закупки иностранного программного обеспечения</i>, в том числе в составе программно-аппаратных комплексов..., в целях его</p>

Нормативный документ	Положения
информационной инфраструктуры Российской Федерации»	использования на принадлежащих им значимых объектах критической информационной инфраструктуры... <b>б)</b> с 1 января 2025 г. органам государственной власти, <i>заказчикам</i> запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.
Требования к программному обеспечению, в том числе в составе программно-аппаратных комплексов..., утвержденных постановлением Правительства РФ от 22.08.2022 № 1478	<p><b>Пункт 1.</b> Программное обеспечение, в том числе в составе программно-аппаратных комплексов, используемое органами государственной власти, <i>заказчиками</i>, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, <i>должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных</i> или в единый реестр программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации.</p> <p><b>Пункт 2.</b> Программное обеспечение, предназначенное для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации... должно соответствовать настоящим требованиям и требованиям, установленным ФСТЭК России и (или) ФСБ России в пределах их полномочий, что должно быть подтверждено соответствующим документом (<i>сертификатом</i>).</p>

## 5. Информационные системы финансовых организаций (банков)

Перечень и положения нормативно-правовых актов, определяющих использование сертифицированных средств защиты информации при обработке информации в информационных системах финансовых организаций (банков) приведены в таблице 5.

Таблица 5.

Нормативный документ	Положения
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	<b>Статья 16. Защита информации</b> <b>Пункт 2.</b> Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.
ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (утв. и введен в действие Приказом Росстандарта от 08.08.2017 N 822-ст).	<b>Базовый состав мер по реализации процесса системы защиты информации</b> Мера защиты информации <b>РЗИ.11</b> Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 4 класса ( <i>для уровня защиты информации 1 (усиленный) – примечание ООО «САФИБ»</i> ) Мера защиты информации <b>РЗИ.12</b> Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 5 класса ( <i>для уровня защиты информации 2 (стандартный) – примечание ООО «САФИБ»</i> ) Мера защиты информации <b>РЗИ.13</b> Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса ( <i>для уровня защиты информации 3 (минимальный) – примечание ООО «САФИБ»</i> ) <i>Примечание. Меры РЗИ.11-РЗИ.13 применяются «В случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации».</i>  <b>Базовый состав мер защиты информации на этапе «Создание (модернизация) АС»</b> Мера защиты информации <b>ЖЦ.8</b> Применение прикладного ПО АС, сертифицированного



Нормативный документ	Положения
	<p>на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недеklarированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3 (см. примечание).</p> <p><i>Примечание. В случаях, предусмотренных нормативными актами Банка России, и (или) если в соответствии с моделью угроз и нарушителей безопасности информации финансовой организации, угрозы, связанные с наличием уязвимостей и недеklarированных возможностей в прикладном ПО АС, признаны актуальными.</i></p>
<p>Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»</p>	<p><b>Пункт 4.1.</b> В отношении прикладного программного обеспечения автоматизированных систем и приложений, не указанных в абзаце первом настоящего подпункта, кредитные организации должны <i>самостоятельно определять необходимость сертификации или анализа уязвимостей</i> и контроля отсутствия недеklarированных возможностей.</p>
<p>Положение Банка России от 17.04.2019 N 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»</p>	<p><b>Пункт 9.</b> Некредитные финансовые организации, не указанные в абзаце первом настоящего пункта, должны <i>самостоятельно определять необходимость сертификации или анализа уязвимостей</i>.</p> <p>В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего подпункта, некредитные финансовые организации должны <i>самостоятельно определять необходимость сертификации или анализа уязвимостей</i>.</p>

Нормативный документ	Положения
	<p><b>Пункт 8.2.</b> <i>Доступ к средствам управления и администрирования серверных компонентов виртуализации рекомендуется осуществлять с использованием СЗИ от несанкционированного доступа, прошедшим оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.</i></p> <p><i>Примечание ООО «САФИБ»: ПК «Ассистент» позволяет осуществлять доступ к средствам управления и администрирования серверных компонентов виртуализации, перечень поддерживаемых операционных систем, в том отечественных ОС, приведен в эксплуатационной документации.</i></p> <p><b>Пункт 13.6.</b> <i>Для организации защищенного доступа к средствам управления и администрирования СХД рекомендуется использовать двухфакторную идентификацию, реализуемую СЗИ от несанкционированного доступа, прошедшими оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.</i></p> <p><i>Примечание ООО «САФИБ»: ПК «Ассистент» содержит функционал двухфакторной идентификации.</i></p>



## 6. Информационные системы медицинских организаций

Перечень и положения нормативно-правовых актов, определяющих использование сертифицированных средств защиты информации при взаимодействии информационных систем медицинских организаций, участвующих в информационном взаимодействии с единой государственной информационной системой в сфере здравоохранения, информационными системами в сфере здравоохранения и медицинскими организациями приведены в таблице 6.

Таблица 6.

Нормативный документ	Положения
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	<b>Статья 16. Защита информации</b> <b>Пункт 2.</b> Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.
Постановление Правительства РФ от 12.04.2018 N 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями»	<b>Пункт 7.</b> Для взаимодействия с единой системой и информационными системами в сфере здравоохранения <i>иные информационные системы</i> , обрабатывающие персональные данные и (или) сведения, составляющие врачебную тайну, помимо требований, предусмотренных пунктом 5 настоящих Правил, должны: з) обеспечивать применение <i>сертифицированных</i> по требованиям безопасности информации средств защиты информации;

## 7. Сертификат соответствия ФСТЭК России № 4162 выдан 26.08.2019

«Система удаленного мониторинга и управления «Ассистент»» может применяться в составе:

- системы защиты информации государственных информационных систем до 1 класса защищенности (включительно), определенного в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17;

- системы защиты персональных данных до 1 уровня защищенности (включительно), определенного в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

- системы защиты информации автоматизированных систем управления производственными и технологическими процессами до 1 класса защищенности (включительно), определенного в соответствии с Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденными приказом ФСТЭК России от 14 марта 2014 г. № 31;

- системы защиты информации значимых объектов критической информационной инфраструктуры Российской Федерации до 1 категории (включительно), определенной в соответствии с Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

Встроенное средство защиты от несанкционированного доступа к информации программного комплекса «Система удаленного мониторинга и управления «Ассистент» версия 2» соответствует требованиям по безопасности информации **по 4 уровню доверия** и реализует следующие технические меры по обеспечению безопасности информации (персональных данных):

- в части идентификации и аутентификации субъектов доступа и объектов доступа: **ИАФ.1 - ИАФ.5, ИАФ.7;**

- в части управления доступом субъектов доступа к объектам доступа: **УПД.1 - УПД.6, УПД.13;**

- в части регистрации событий безопасности: **РСБ.1 - РСБ.4;**

- в части обеспечения целостности информационной системы и информации: **ОЦЛ.1.**

## **Заключение**

При организации удаленного доступа необходимо выполнить анализ информационных систем (информационных систем персональных данных) с целью определения необходимости использования, в соответствии с действующим законодательством, сертифицированного программного продукта.

Использование ПК «Ассистент» позволяет снизить расходы на создание системы защиты информации, а его использование в составе информационной системы будет соответствовать действующему законодательству Российской Федерации в области защиты информации и импортозамещения. Будут нейтрализованы актуальные угрозы безопасности информации. Нет необходимости принятия компенсирующих мер за счет использования реализованных в программном обеспечении функций безопасности. Будет предоставлена гарантийная техническая поддержка предприятия-производителя. Срок эксплуатации изделия - 5 лет.

## **Список использованных источников**

1. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
6. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
7. Постановление Правительства РФ от 12.04.2018 N 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями».
8. Постановление Правительства РФ от 22.08.2022 № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов...».
9. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
10. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
11. 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».
12. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
13. Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».
14. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых

организаций. Базовый состав организационных и технических мер (утв. и введен в действие Приказом Росстандарта от 08.08.2017 N 822-ст).

15. Положение Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

16. Положение Банка России от 17.04.2019 N 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».