ДЕПАРТАМЕНТ СМОЛЕНСКОЙ ОБЛАСТИ ПО ЗДРАВООХРАНЕНИЮ

пл. Ленина, д. 1, г. Смоленск, 214008,
e-mail: info@zdrav-smolensk.ru.
тел.: (4812) 29-22-55, (4812) 29-22-01,
факс: (4812) 38-67-58

от 07.07.2022 № 11103

на № _____ от _____

Руководителям медицинских организаций частной системы здравоохранения Смоленской области

Уважаемые руководители медицинских организаций!

Департамент Смоленской области по здравоохранению (далее – Департамент) во исполнение письма Министерства здравоохранения Российской Федерации от 20.06.2022 №18-5/1561 и с целью реализации мероприятий федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» национального проекта «Здравоохранение» в части достижения результата «Медицинские организации частной системы здравоохранения используют медицинские информационные системы, соответствующие требованиям Минздрава России, обеспечивают информационное взаимодействие с подсистемами ЕГИСЗ и с другими отраслевыми информационными системами, включая государственные информационные системы в сфере здравоохранения субъектов Российской Федерации, при оказании медицинской помощи гражданам, и вносят в названные системы сведения об оказанной гражданам медицинской помощи» сообщает следующее.

Согласно ст. 91 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» в информационных системах в сфере здравоохранения осуществляется сбор, хранение, обработка и предоставление информации об организациях частной системы здравоохранения и об осуществлении медицинской и иной деятельности в сфере охраны здоровья. Согласно пп. III-VI Приложения № 1 к Положению о Единой государственной информационной системе в сфере здравоохранения, утвержденному Постановлением Правительства Российской Федерации от 09.02.2022 № 140 «О единой государственной информационной системе в сфере здравоохранения», установлены сроки предоставление информации в подсистемы ЕГИСЗ для медицинских организаций частной системы здравоохранения.

Дополнительно сообщаем, что в соответствии с порядком подключения информационных систем в сфере здравоохранения к подсистемам ЕГИСЗ

медицинские информационные системы (далее – МИС) медицинских организаций частной системы здравоохранения могут подключаться к подсистемам ЕГИСЗ следующими способами:

- посредством взаимодействия с информационной системой в сфере здравоохранения субъекта Российской Федерации (далее – ИС субъекта РФ);
- через иные информационные системы;
- путем прямого подключения.

При этом медицинские организации частной системы здравоохранения должны:

- обеспечивать защиту информации, содержащейся в МИС, посредством применения организационных и технических мер защиты информации, а также посредством осуществления контроля за эксплуатацией МИС;
- обеспечивать защиту информации, получаемую из ИС субъекта РФ посредством МИС, в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, установленными Федеральной службой по техническому и экспортному контролю в соответствии с ч. 5 ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- осуществлять информационное взаимодействие МИС с ИС субъекта РФ /ЕГИСЗ посредством защищенного способа передачи данных.

В связи с изложенным Департамент просит в кратчайшие сроки провести необходимую организационную работу по подключению к ИС субъекта РФ /ЕГИСЗ в целях передачи сведений, установленных действующим законодательством Российской Федерации.

О сроках готовности к подключению к ИС субъекта РФ /ЕГИСЗ сообщить в срочном порядке по эл. адресам в адрес Департамента (info@zdrav-smolensk.ru) и копией в ОГАУЗ «СОМИАЦ» (somiac@mail.ru).

И.о. начальника Департамента **И.М. Веселова**

Исп. Никитина Ирина Николаевна
(4812) 29-22-79

Департамент Смоленской области по здравоохранению

УТВЕРЖДАЮ

Начальник Департамента Смоленской области по здравоохранению

_____ О.С. Стунжас

« _____ » _____ 2022 г.

ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ информационной системой в сфере здравоохранения Смоленской области (ПОИБ ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»)

ПОРЯДОК ПОДКЛЮЧЕНИЯ

Действует с « _____ » _____ 20__ г.

Смоленск
2022

СОКРАЩЕНИЯ И НАИМЕНОВАНИЯ

АРМ	- автоматизированное рабочее место;
БД	- сервера с базами данных
ГИС	- государственная информационная система;
ИС	- информационная система;
ИСПДн	- информационная система персональных данных;
Внешний пользователь	- сотрудник частной медицинской организации
Оператор	- Департамент Смоленской области по здравоохранению
ЗСВ	- защита среды виртуализации;
ЛВС	- локальная вычислительная сеть;
МЭ	- межсетевой экран;
НДВ	- недекларированные возможности;
НСД	- несанкционированный доступ;
ПДн	- персональные данные;
ПОИБ	- подсистема обеспечения информационной безопасности;
ЗСПД ОЗ СО	- Защищенная сеть связи и передачи данных органов здравоохранения Смоленской области;
САЗ	-средство анализа защищенности;
САВ	-средство антивирусной защиты;
СОВ	- средство обнаружения вторжений;
СЗИ	- средство защиты информации;
СКЗИ	- средство криптографической защиты информации;
ФСТЭК России	- Федеральная служба по техническому и экспортному контролю;
ФСБ России	- Федеральная служба безопасности.

АНОТАЦИЯ

Настоящие технические условия определяют требования к подключению автоматизированного рабочего места (далее – АРМ) Пользователя к информационной системой в сфере здравоохранения Смоленской области (далее – ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»).

Данный документ предназначен для сотрудников медицинских организаций частной системы здравоохранения Смоленской области, отвечающих за подключение АРМ Пользователей к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», а также для Администратора безопасности ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ». Сотрудник, отвечающий за подключение к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», должен иметь квалификацию системного администратора (технического специалиста), обладать знаниями и опытом в области конфигурирования, эксплуатации и управления персональным компьютером и сетевым оборудованием, а также знаниями в области информационной безопасности.

ВВЕДЕНИЕ

На основании Постановления Правительства Российской Федерации «О единой государственной информационной системе в сфере здравоохранения» от 09.02.2022 № 140 Департаментом Смоленской области по здравоохранению (далее – Оператор) создается ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»

Согласно ст. 91 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ в информационных системах в сфере здравоохранения осуществляется сбор, хранение, обработка и предоставление информации об организациях частной системы здравоохранения и об осуществлении медицинской и иной деятельности в сфере охраны здоровья. Согласно п. 3 Положения о лицензировании медицинской деятельности (за исключением указанной деятельности, осуществляемой медицинскими организациями и другими организациями, входящими в частную систему здравоохранения, на территории инновационного центра «Сколково»), утвержденного Постановлением Правительства Российской Федерации от 01.06.2021 № 852, лицензирование медицинской деятельности осуществляют, в том числе, уполномоченные органы исполнительной власти (далее – ОИВ) субъектов Российской Федерации, кроме того, согласно пп. «е» п. 6 лицензионным требованием, предъявляемым к лицензиату при осуществлении им медицинской деятельности, является требование размещения информации в ЕГИСЗ.

В соответствии с п. 8 Приказа ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г №21 в ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» для обеспечения защиты информации с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее – машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

Требования настоящих технических условий устанавливают состав, содержание, порядок выполнения работ по подключению АРМ внешних пользователей, а также состав программно-технических средств, в том числе средств защиты информации, необходимых для организации защищенного взаимодействия АРМ внешних пользователей с БД ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ».

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. Общее описание информационного обмена

Обмен информацией между АРМ внешних пользователей и БД ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» осуществляется в электронном виде с использованием защищенной сети передачи данных органов здравоохранения Смоленской области (ЗСПД ОЗ СО).

В ЗСПД ОЗ СО для защиты информации конфиденциального характера используются сертифицированные шифровальные (криптографические) средства на базе продуктов семейства ViPNet (сеть 1558).

При осуществлении информационного обмена основными сетевыми телекоммуникационными протоколами, являются протоколы семейства TCP/IP.

1.2. Организационные требования.

Организация подключения АРМ внешнего пользователя к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» должна осуществляться в соответствии с:

- требованиями нормативно-правовых актов Российской Федерации в сфере защиты информации;
- требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (ФСТЭК России, ФСБ России);
- требованиями настоящих Технических условий.

До начала выполнения работ по подключению АРМ внешнего пользователя к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» схема защищенного взаимодействия должна быть согласована с Оператором.

Для обеспечения подключения АРМ к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» в организации должно быть назначено ответственное лицо.

Организация должна разработать и утвердить организационно-распорядительные документы по защите информации в соответствии с требованиями органов регуляторов в области информационной безопасности.

Для выполнения обязанностей операторов персональных данных по организации обработки персональных данных, в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ (далее – 152-ФЗ), необходимо самостоятельно определить состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, в том числе:

- назначить ответственное лицо за организацию обработки персональных данных;
- направить в Управление Роскомнадзора по Смоленской области уведомление об обработке персональных данных. При наличии ранее поданного уведомления (при условии регистрации в реестре) – актуализировать содержащиеся в нем сведения с учетом вводимой в эксплуатацию системой.

- издать документы или актуализировать изменения в документах, определяющие политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 152-ФЗ;

- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

- оценить вред, который может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных 152-ФЗ;

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

- выполнить иные мероприятия предусмотренные 152-ФЗ.

Для обеспечения безопасности информации на АРМ подключаемых к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» необходимо выполнить следующие мероприятия:

- в соответствии с п.15 Постановления Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 №1119 (далее – Постановление Правительства №1119) и п. 17 Приказа ФСБ России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 № 378 (далее – Приказ ФСБ России № 378) для обеспечения защиты персональных данных, назначить структурное подразделение или должностное лицо (работник), ответственных за защиту информации;

- в соответствии с п. 15 Постановления Правительства №1119:

а) организовать режим обеспечения безопасности помещений, в которых размещены АРМ ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечить сохранность носителей персональных данных;

в) утвердить документ, определяющий перечень лиц, доступ которых к

персональным данным, обрабатываемым на АРМ подключенных к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», необходим для выполнения ими служебных (трудовых) обязанностей;

г) необходимо, 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;

д) обеспечить конфиденциальность персональных данных при работе в информационной системе и установить обязанность использования персональных данные только в заранее определенных и законных целях.

- в соответствии с п. 6. Приказа ФСБ России № 378:

а) для выполнения требования, указанного в пп. «а» п. 15 Постановления Правительства №1119, необходимо обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения), лиц, не имеющих права доступа в Помещения, которое достигается путем:

- 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;
- утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- утверждения перечня лиц, имеющих право доступа в Помещения;

б) для выполнения требования, указанного в пп. «б» п. 15 Постановления Правительства №1119необходимо:

- осуществлять хранение 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. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

- осуществлять по экземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров;

- в) для выполнения требования, указанного в пп. «в» п. 15 Постановления Правительства №1119 необходимо внедрить соответствующие СКЗИ:

- разработать и утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым на АРМ ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», необходим для выполнения ими служебных (трудовых) обязанностей;

- поддерживать в актуальном состоянии документ, определяющий перечень

лиц, доступ которых к персональным данным, обрабатываемым на АРМ ИС ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», необходим для выполнения ими служебных (трудовых) обязанностей;

г) для выполнения требования, указанного в пп. «г» п. 15 Постановления Правительства №1119 необходимо внедрить соответствующие средства криптографической защиты информации;

д) для выполнения требования, указанного в п. 15 Постановления Правительства №1119, необходимо утверждение руководителем оператора списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии.

После подключения АРМ пользователя к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», ответственным лицом организации, подключаемой к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», должен быть составлен Акт подключения АРМ пользователя (Приложение №1) в 2-х экземплярах с обязательной отметкой о соответствии требованиям настоящих ТУ. Один экземпляр остается в организации, эксплуатирующей АРМ пользователя, второй экземпляр передается Оператору.

Помещения, в которых расположены АРМ пользователей, должны быть оборудованы средствами вентиляции и кондиционирования воздуха, которые должны соответствовать санитарно-гигиеническими нормам СНиП, устанавливаемым законодательством Российской Федерации.

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

2.1. Перечень мероприятий по подключению АРМ пользователей к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»

Подключение АРМ пользователей к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» производится путем выполнения следующих мероприятий:

- выполнение организационных мероприятий по подключению к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»;
- выполнение технический условий по защите информации на АРМ Пользователя;
- регистрация Пользователей в ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»;
- получение дистрибутивов ключей;
- подключение АРМ пользователей.

2.1.1.Регистрация пользователей.

После проведения мероприятий по организации защиты информации на АРМ Пользователя, организация подает заявку на подключение к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» Оператору.

Оператор централизованно создает учетные записи на пользователя системы, и передает атрибуты доступа на защищенном носителе USB-токен JaCarta.

2.1.2. Получение дистрибутива ключей.

За ключевой информацией (dst-файл) на ПО ViPNet Client (сеть 1558) ответственное лицо обращается в областное государственное автономное учреждение здравоохранения «Смоленский областной медицинский информационно-аналитический центр» (далее – ОГАУЗ «СОМИАЦ») за получением дистрибутива ключей. Заявка оформляется по форме Приложение 2.

2.1.3. Подключение АРМ пользователей.

Подключение организации к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» выполнятся после письменного уведомления Оператора о выполнении технических требований к подключению АРМ внешних пользователей к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ», в виде копии акта об установке и настройке СЗИ применяемых на АРМ пользователя.

2.2. Технические требования к подключению АРМ пользователей к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»

2.2.1. Требования к СЗИ, применяемым на АРМ к ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ».

На АРМ организации должны использоваться средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, обеспечивающее:

- доверенную загрузку АРМ (Аппаратно-программный модуль доверенной загрузки «Соболь»);
- защиту от несанкционированного доступа (СЗИ от НСД Secret Net Studio 8.3);
- антивирусную защиту ПК («Kaspersky Endpoint Security 10 for Windows» с лицензией Kaspersky Systems Management);
- средство криптографической защиты каналов связи ПК ViPNet Client 4 (сеть 1558).

Все выше перечисленные СЗИ должны быть настроены в соответствии с требованиями руководящих документов в области информационной безопасности и защиты персональных данных.

2.22. Требования к АРМ пользователя.

На АРМ пользователя должна быть установлена только одна из перечисленных ОС.

В BIOS должен быть установлен одни вариант загрузки ОС - с жесткого диска, все альтернативные варианты загрузки должны быть отключены, в том числе сетевая загрузка.

На АРМ пользователя должны быть выполнены корректные настройки часового пояса, даты и времени.

Если на АРМ пользователя установлена ОС Windows, локализация которой

отличается от русской, то для правильного отображения кириллицы в интерфейсе ПО ViPNet Client необходимо установить поддержку кириллицы для программ, не поддерживающих Unicode.

Запрещаться пользоваться отладочными версиями ОС, такими как Debug/Checked Build, а также устанавливать средства отладки и трассировки программного обеспечения.

На АРМ пользователя должны быть отключены сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT).

Для проведения работ по защите информации в ходе создания и эксплуатации АРМ внешних пользователей в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие:

- лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации проектирования в защищенном исполнении средств и систем информатизации, установки, монтажа, средств защиты информации;
- лицензию ФСБ России на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации.

3. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ

Ответственность за соблюдение требований настоящих ТУ, обеспечение защиты информации в ходе эксплуатации АРМ внешних пользователей, а также ответственность за соблюдение требований к эксплуатации средств защиты информации и СКЗИ в составе системы защиты информации АРМ внешних пользователей, лежит на владельцах подключаемых АРМ внешних пользователей.

Оператор имеет право проводить проверки реализации схем подключения. В случае выявления нарушений требований настоящих ТУ, Оператор немедленно производит отключение соответствующего АРМ внешнего пользователя от ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ».

4. ОТВЕТСТВЕННОСТЬ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ»

Ответственность за правомерность осуществления ведения обработки персональных данных в ИС «СЗ СМОЛЕНСКОЙ ОБЛАСТИ» несет каждый оператор, имеющий к ней доступ и производящий те или иные действия с персональными данными субъектов персональных данных. Виновные лица будут нести персональную ответственность.

Приложение №1

АКТ
о подключении АРМ пользователя к информационной системе
«СЗ СМОЛЕНСКОЙ ОБЛАСТИ»

г. Смоленск «___» _____ 202_ года

Департамент Смоленской области по здравоохранению, именуемое в дальнейшем «Оператор», в лице _____, действующего на основании _____, с одной стороны и _____, именуемое в дальнейшем «Участник», в лице _____, действующего на основании _____, с другой стороны, составили настоящий акт о подключении автоматизированного рабочего места Участника к информационной системе «СЗ СМОЛЕНСКОЙ ОБЛАСТИ».

Участник подтверждает выполнение типовых требований (технических условий) для подключения автоматизированных рабочих мест пользователей к информационной системе «СЗ СМОЛЕНСКОЙ ОБЛАСТИ».

Участник подтверждает соблюдение требований органов регуляторов в области информационной безопасности по режиму обработки данных на подключаемом автоматизированном рабочем месте.

ОПЕРАТОР	ПОЛЬЗОВАТЕЛЬ
_____/_____	_____/ _____

Приложение №2

(Оформляется на бланке Организации заявителя)

Директору областного государственного автономного учреждения здравоохранения «Смоленский областной медицинский информационно-аналитический центр»

А.А. Кирпенко

ЗАЯВЛЕНИЕ
на создание абонентского пункта сети ViPNet сеть № 1558

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность, фамилия, имя, отчество)

действующего на основании _____
просит создать абонентский пункт и изготовить дистрибутив ключей сети ViPNet сеть № 1558 для своего уполномоченного представителя в соответствии с указанными в настоящем заявлении данными:

Наименование юридического лица	
ФИО уполномоченного лица	
Сведения о документе, удостоверяющим личность (наименование, серия, номер, кем и когда выдан)	
Подразделение	
Должность	
Место нахождения (адрес установки абонентского пункта)	

Настоящим, _____
(фамилия, имя, отчество субъекта персональных данных)

даю свое согласие ОГАУЗ «СОМИАЦ» (214000, г. Смоленск, ул. Тенишевой, д. 9) на обработку (сбор, запись, систематизация, накопление, хранение, уточнение, извлечение, использование, блокирование, удаление, уничтожение) смешанным способом моих персональных данных, содержащихся в данном заявлении, с целью создания абонентского пункта сети ViPNet № 1558.

Мои персональные данные (Ф.И.О., должность, место работы, и т.д.), содержащиеся в заявлении, считать общедоступными.

Настоящее согласие может быть отозвано мной путем подачи заявления в письменном виде в адрес ОГАУЗ «СОМИАЦ».

Настоящее заявление заполняется собственноручно субъектом персональных данных.

Уполномоченное лицо _____ _____

(подпись) (инициалы / фамилия)

Руководитель организации _____ _____
(подпись) (инициалы / фамилия)

М.П. «____»_____ 20 ___ г.