УТВЕРЖДАЮ

Директор КГБУЗ «Алтайский краевой медицинский информационно-аналитический центр»

_____В.Г.Азанов

«12» марта 2021

РЕГЛАМЕНТ
подключения к государственной информационной системе «Здравоохранение»

г. Барнаул 2021

Перечень сокращений, используемых в настоящем Регламенте

АРМ	Автоматизированное рабочее место
ГИС	Государственная информационная система
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
ТС	Технические средства
ТУ	Технические условия
ЦОД	Центр обработки данных
ЭД	Эксплуатационная документация

АННОТАЦИЯ

Регламент подключения к ГИС «Здравоохранение» (далее – «Регламент») определяет требования и условия подключения организаций к государственной информационной системе, расположенной в КГБУЗ «АКМИАЦ».

Требования Регламента распространяются на АРМ и ЛВС организаций, подключаемых (имеющих подключение) к центру обработки данных КГБУЗ «АКМИАЦ».

ВВЕДЕНИЕ

В соответствии с положениями Федерального закона Российской Федерации от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» в КГБУЗ «АКМИАЦ» функционирует государственная информационная система, обеспечивающая работу по различным направлениям, связанным с обеспечением охраны здоровья населения в Алтайском крае и функционированием медицинских учреждений.

ЦОД ГИС «Здравоохранение» аттестован на соответствие требованиям по обеспечению безопасности информации, не составляющей государственную тайну, при ее обработке в государственных информационных системах.

Требования Регламента устанавливают состав, содержание, а также порядок выполнения работ по подключению АРМ и ЛВС организаций, а также состав программно-технических средств, в том числе средств защиты информации, необходимых для организации защищенного взаимодействия АРМ и ЛВС организаций с ЦОД ГИС «Здравоохранение».

Настоящий Регламент разработан во исполнение следующих нормативно-правовых актов:

Федеральный закон Российской Федерации от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

постановление Правительства Российской Федерации от 01.11.2012

№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1 Назначение информационной системы

ГИС «Здравоохранение» создана и используется для исполнения возложенных на Министерство здравоохранения Алтайского края полномочий. ГИС функционирует в распределенной ЛВС, объединяющей АРМ специалистов медицинских учреждений, АРМ разработчиков, участвующих в процессах обмена информацией.

ГИС «Здравоохранение» состоит из серверной части и рабочих мест пользователей, (специалистов медицинских учреждений Алтайского края и разработчиков модулей ГИС «Здравоохранение»), участвующих в процессах обмена информацией. Серверная часть функционирует на базе ЦОД КГБУЗ «АКМИАЦ», который расположен по адресу: 656031, г. Барнаул, пр. Красноармейский, д. 95-а.

1.2 Структура ГИС «Здравоохранение»

Структура ГИС «Здравоохранение» включает:

комплекс программных и технических средств сбора, обработки, хранения и передачи информации, содержащейся в ГИС «Здравоохранение» (серверный сегмент);

комплексы программных и технических средств сбора, обработки, хранения и передачи информации, содержащейся в ГИС «Здравоохранение» (сегмент организации);

комплекс программных и технических средств системы защиты информации ГИС «Здравоохранение» серверного сегмента;

комплекс программных и технических средств системы защиты информации ГИС «Здравоохранение» сегмента медицинского учреждения;

телекоммуникационную инфраструктуру, в том числе каналы передачи данных.

1.3 Участники информационного обмена

Участниками информационного обмена являются:

Министерство здравоохранения Алтайского края (владелец информационной системы);

КГБУЗ «АКМИАЦ» (оператор информационной системы);

Медицинские организации (пользователи информационной системы)

Разработчики модулей ГИС.

1.4 Классификация ГИС

В соответствии с Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» ГИС «Здравоохранение» имеет 2 класс защищенности (К2).

1.5 Общее описание информационного обмена

Обмен информацией между ЦОД ГИС «Здравоохранение» и АРМ и ЛВС организаций осуществляется в электронном виде с использованием сертифицированных шифровальных (криптографических) средств (сеть ViPNet № 2495) по сетям связи общего пользования (сети Интернет).

2. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

2.1 Общие требования

Для организации защищенного взаимодействия с ЦОД ГИС «Здравоохранение» должны быть выполнены организационные и технические мероприятия, для приведения системы защиты информации АРМ и ЛВС организаций в соответствие требованиям по защите информации в ГИС.

Для обеспечения защиты информации, содержащейся на АРМ и ЛВС организаций, должны применяться средства защиты информации, прошедшие процедуру оценки соответствия в форме сертификации на соответствие требованиям по безопасности информации применимым к государственным информационным системам 2 класса защищенности.

Для проведения работ по защите информации в ходе создания и эксплуатации АРМ и ЛВС организаций 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.

2.2 Требования к защите АРМ и ЛВС организаций

В соответствии с нормативно-правовыми актами в сфере защиты информации в ЦОД ГИС «Здравоохранение» и АРМ и ЛВС организаций приняты меры по защите информации, в соответствии с требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В рамках системы защиты информации ГИС «Здравоохранения» реализуются организационные и технические меры защиты информации на АРМ и ЛВС организации и в ЦОД ГИС «Здравоохранение».

Для реализации технических мер защиты информации необходимо применение средств защиты информации.

Для защиты серверов под управлением ОС семейства Windows:

СЗИ от НСД для ОС Windows систем и терминальных серверов (например, Secret Net Studio, Dallas Lock 8.0-К и другие);

средство доверенной загрузки (например, программно-аппаратный комплекс «Соболь», СДЗ Dallas Lock и другие);

система антивирусной защиты (например, Kaspersky Endpoint Security, Dr. Web Enterprise Security Suite и другие).

Для защиты серверов под управлением ОС семейства Linux:

СЗИ от НСД для Linux систем (например, Secret Net LSP, Dallas Lock Linux и другие);

средство доверенной загрузки (например, программно-аппаратный комплекс «Соболь», СДЗ Dallas Lock и другие);

система антивирусной защиты (например, Kaspersky Endpoint Security, Dr. Web Enterprise Security Suite и другие).

Защита среды виртуализации:

средство защиты виртуальных сред (в этом случае необходимо добавление в структуру системы защиты физического АРМ или сервера для установки сервера авторизации средства защиты виртуальных сред, например, vGate R2);

средство доверенной загрузки (на гипервизор) (например, программно-аппаратный комплекс «Соболь», СДЗ Dallas Lock и другие);

система антивирусной защиты (на каждый виртуальный сервер) (например, Kaspersky Endpoint Security, Dr. Web Enterprise Security Suite и другие);

система антивирусной защиты для виртуальных сред (на гипервизор) (например, Kaspersky Security для виртуальных сред, Dr. Web Enterprise Security Suite и другие).

Средство анализа уязвимостей - действие данного СЗИ распространяется на организацию посредством поиска уязвимостей (например, Сканер-ВС и другие).

Система обнаружения вторжений – устанавливается на уровне ЦОД, с целью централизованного обнаружения атак на ГИС (например, ViPNet IDS).

Защита каналов связи:

криптографический шлюз и межсетевой экран (например, ViPNet Client, ViPNet Coordinator HW100, ViPNet Coordinator HW1000, ViPNet Coordinator HW2000);

Защита стационарного АРМ (компьютера) (под управлением ОС семейства Windows):

СЗИ от НСД для Windows систем (например, Secret Net Studio, Dallas Lock 8.0-K и другие);

средство доверенной загрузки (например, программно-аппаратный комплекс «Соболь», СДЗ Dallas Lock и другие);

система антивирусной защиты (например, Kaspersky Endpoint Security, Dr. Web Enterprise Security Suite и другие).

Защита «тонкого клиента» с загрузкой ОС по ЛВС с TFTP сервера медицинского учреждения:

аппаратный ключ (Токен) (для обеспечения двухфакторной аутентификации).

Виртуальные сервер с использованием сертифицированной ОС (на базе ядра Linux), с применением системы виртуализации:

средство доверенной загрузки (например, программно-аппаратный комплекс «Соболь», СДЗ Dallas Lock и другие);

средство антивирусной защиты (совместимое с сертифицированной ОС).

В организации разрабатывается и утверждается комплект организационной распорядительной документации, в части обеспечения безопасности персональных данных и ГИС «Здравоохранение». Руководители организаций назначают лиц, ответственных за внесение сведений в АРМ и ЛВС организаций, а также лиц, ответственных за обеспечение мер по защите информации, обрабатываемой в АРМ и ЛВС организаций.

Для взаимодействия АРМ и ЛВС организации с ЦОД ГИС «Здравоохранение», подключаемое медицинское учреждение должно иметь действующий аттестат, подтверждающий соответствие требованиям по обеспечению безопасности информации, не составляющей государственную тайну, при ее обработке в государственных информационных системах класса К2.

После реализации необходимых мер защиты информации медицинское учреждение присылает заявку в КГБУЗ «АКМИАЦ» на подключение к ГИС «Здравоохранение».

2.3 Специальные требования

Помещения для размещения технических средств АРМ и ЛВС организаций должны удовлетворять требованиям ТУ и ЭД на данные средства.

Схема подключения АРМ и ЛВС организаций к ЦОД ГИС «Здравоохранение», а также необходимые для их корректного функционирования настройки должны быть предварительно согласованы с КГБУЗ «АКМИАЦ».

Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ должны выполняться в соответствии с требованиями ТУ и ЭД на данные средства.

Эксплуатация средств защиты информации и СКЗИ должна осуществляться в соответствии с организационно-технической, организационно-распорядительной документацией и ЭД на систему защиты информации АРМ и ЛВС организации.

Обеспечение защиты информации в ходе эксплуатации АРМ и ЛВС организации осуществляется её владельцем в соответствии с организационно-технической, организационно-распорядительной документацией и ЭД на систему защиты информации АРМ и ЛВС организации, настоящим Регламентом и нормативно-техническими документами РФ в сфере защиты информации.