УТВЕРЖДАЮ
Директор
ГКУ ТО «ЦИТТО»

_____ А.Р. Усманов

«__» _____ 2019 г.

Регламент
технических требований
на подключение автоматизированных рабочих мест
к государственной информационной системе
«УРМО ТО»

г. Тюмень, 2019

1. Обозначения и сокращения

УРМО ТО – управление ресурсами медицинских организаций Тюменской области;
ГИС – государственная информационная система;
ИС – информационная система;
АРМ – автоматизированное рабочее место;
ЭП – электронная подпись.

1. Общие положения

1.1. Настоящий Регламент определяет технические требования на подключение АРМ к государственной информационной системе «УРМО ТО» (далее - ГИС), не содержащей сведения, составляющие государственную тайну.

2. Техническое оснащение АРМ.

В качестве АРМ ГИС «УРМО ТО», используется персональный компьютер (допускается настольное и портативное использование), возможно использование серверов или специализированных устройств.

Для выполнения подключения к ГИС, АРМ пользователя должны быть подключены к сетям связи общего пользования (Интернет) или виртуальной частной сети (VPN) с доступом к ЦОД Правительства Тюменской области.

Скорость подключения – не ниже 10 Мбит/с, интерфейс – Ethernet 10/100.

На АРМ пользователя ГИС должна быть установлена операционная система не ниже Windows 7 либо ОС семейства AltLinux.

На АРМ пользователя ГИС должно быть установлено программное обеспечение КриптоПро CSP не ниже версии 4.0.

3. Информационная безопасность АРМ.

С целью обеспечения выполнения требований законодательства РФ, предъявляемых к государственным информационным системам, для АРМ пользователя, подключаемым к ГИС, должны быть реализованы мероприятия с учетом разработанной модели угроз:

1) Помещения, в которых размещаются АРМ, взаимодействующие с ГИС, должны обеспечивать конфиденциальность проводимых работ.

2) Должен быть исключен доступ (физический и/или удаленный) к компьютеру третьих лиц, не имеющих полномочий для работы в ГИС.

3) На АРМ должна быть активирована подсистема регистрации событий информационной безопасности и включена автоматическая блокировка экрана после ухода работника с рабочего места.

4) Необходимо использовать антивирусное программное обеспечение, с обновлением вирусных баз не реже раза в сутки и проведением периодических антивирусных проверок компьютеров сертифицированными ФСТЭК России средствами.

5) Необходимо исключить прямое подключение АРМ, взаимодействующих с ГИС, к сетям общего пользования (Интернет) – АРМ должны располагаться за средствами межсетевого экранирования (фаервола) во внутренней сети пользователя или в демилитаризованной зоне.

6) Входящий и исходящий сетевой трафик подключаемых АРМ должен контролироваться (фильтроваться) средствами межсетевого экранирования;

7) Необходимо отключить на АРМ автозагрузку со сменных носителей (дискет, флэш-накопителей, оптических дисков) как потенциальный источник угроз.

8) Должны регулярно устанавливаться обновления операционной системы.

9) Для обеспечения целостности и юридической значимости передаваемой информации в процессе информационного взаимодействия должны использоваться сертифицированные ФСБ России средства криптографической защиты информации, реализующие функционал ЭП.

10) Ключевые носители ЭП и АРМ, взаимодействующие с ГИС и содержащие ключи ЭП, в организации пользователя берутся на поэкземплярный учет в выделенных для этих целей журналах.

11) Доступ к ключам ЭП должен быть ограничен на уровне операционной системы и прикладной программы только учетными записями пользователей, имеющих прямое отношение к обработке ключевой информации, и запрещен по сети;

12) Сменный носитель с ключевой информацией должен использоваться только владельцем сертификата ключа проверки электронной подписи либо лицом, уполномоченным на использование такого сменного носителя, и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик). Хранение ключевых носителей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования, применение.

13) Подключение ключевых носителей к АРМ, взаимодействующим с ГИС, допускается только на время работы с системой.

14) Должны быть настроены механизмы аудита доступа и оповещения о попытках несанкционированного доступа к ключам ЭП, хранящимся на АРМ, взаимодействующих с ГИС.

15) При транспортировке ключевых носителей ЭП, АРМ с ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

16) Уничтожение ключевой информации осуществляется в соответствии с процедурами, принятыми у пользователя для уничтожения конфиденциальной информации.

4. Защита каналов связи.

Для обеспечения взаимодействия удаленных АРМ с ГИС необходимо выполнение комплекса мер по защите каналов связи на неконтролируемых участках.

Для доступа АРМ пользователя к ГИС могут быть использованы различные транспортные сети с использованием стека протоколов TCP/IP, в том числе публичные – Интернет.

При использовании публичных сетей для доступа к ГИС Тюменской области необходимо применять сертифицированное РФ программное обеспечение криптографической защиты каналов связи уровня не ниже КС2.

Удаленный доступ к ГИС производится по протоколу SSL VPN с использованием в соответствии с порядком, размещенным на сайте оператора (www.citto.ru).