**Требования по защите информации при подключении пользователей к государственной информационной системе Республики Карелия «Региональная контрактная система»**

 Настоящие Требования установлены на основании документа «Техническое задание. Подсистема обеспечения информационной безопасности. Государственная информационная система Республики Карелия «Региональная контрактная система», согласованного с ФСТЭК России и определяют меры защиты информации обязательные при подключении и работе в государственной информационной системе Республики Карелия «Региональная контрактная система» (далее - ГИС «РКС»).

Для работы пользователей с ГИС «РКС» могут применяться стационарные автоматизированные рабочие места (далее - АРМ **)**, а также ноутбуки (далее – МУ), обеспечивающие возможность работы пользователей через интернет-браузер по каналам связи сети общего пользования Интернет.

**Общие требования**

Применяемое АРМ и МУ должно быть выдано пользователю работодателем для работы и закреплено за ним или являться личным устройством и применяться только им самим [ЗНИ 1,2, ЗИС.30 [1]];В отношении применяемых АРМ и МУ пользователем самостоятельно обеспечивается исключение возможности несанкционированного ознакомления с информацией посторонних лиц, включая применение таких мер как сокрытие информации, выводимой на экран, и блокировка экрана в случае длительной неактивности. Доступ пользователя к АРМ и МУ должен осуществляться только после прохождения аутентификации [ЗНИ 3, УПД.10, ЗТС.4];

На АРМ и МУ должно отсутствовать программное обеспечение, реализующее функции удаленной активации видеокамер, микрофонов и иных периферийных устройств. Устройство должно иметь возможность реализовать запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и провести оповещение пользователя об активации таких устройств, в том числе путем сигнализации, индикации [ЗИС.5];

Применяемая на АРМ и МУ операционная система должна быть лицензионной, официально сопровождаемой разработчиком и не модифицированной. Обновления безопасности и системные обновления, выпускаемые разработчиком, должны быть своевременно установленными [ОПС.2, 3, АНЗ.1.2];

В операционной системе должны вестись стандартные электронные журналы регистрации событий (включены по умолчанию); синхронизируются и применяются актуальные для местоположения пользователя часовой пояс, дата и время [РСБ];

Работа в ГИС «РКС» разрешена только с использованием отечественного интернет-браузера, поддерживающего протокол защиты транспортного уровня TLS версии 1.3. Интернет-браузер должен быть последней актуальной версии и иметь возможность получать автоматические обновления [ОПС.2, 3, АНЗ.2, ЗИС.3];

На АРМ и МУ должно быть установлено и исправно функционировать отечественное антивирусное средство защиты информации [АВЗ.1,2, АНЗ.2,3,4];

На АРМ и МУ должно отсутствовать модифицированное программное обеспечение, способное изменить целостность применяемого антивирусного программного обеспечения и интернет-браузера, а также системных библиотек операционной системы. Антивирусное программное обеспечение и интернет-браузер должны использовать стандартные настройки безопасности, реализованные разработчиком [ОЦЛ.1,3, АНЗ.3,4.];

Для входа в ГИС «РКС» пользователь должен использовать только личные учетные данные (логин и пароль). Передача личных учетных данных кому-либо запрещена. В случае компрометации учетных данных или утери мобильного устройства пользователь должен незамедлительно сменить пароль своей учетной записи в ГИС «РКС» [меры группы ИАФ];

Пользователем принимаются своевременные меры по периодической смене пароля в соответствии с утвержденным «Регламентом подключения и работы в государственной информационной системе «РКС». Доступ к ГИС «РКС» осуществляется в соответствии с предоставленными правами доступа, выданными на основании «Заявка на создание учетной записи пользователя государственной информационной системы Республики Карелия «Региональная контрактная система» [меры группы УПД, АНЗ.5].

**Требования для АРМ и МУ, подключающихся к ГИС «РКС» посредством ведомственных локально-вычислительных сетей**

В организации должна быть установлена и обеспечиваться контролируемая зона, в пределах которой постоянно размещаются АРМ и МУ, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования. В указанной контролируемой зоне исключается неконтролируемое пребывание посторонних лиц, а также посторонних транспортных и технических средств [ЗТС.2,3].

**Требования для МУ, подключаемых к сети «Интернет» за пределами ведомственных локально-вычислительных сетей**

Запрещено подключать МУ к посторонним компьютерам и другим устройствам с целью передачи данных и осуществления зарядки;

Беспроводные соединения Bluetooth, IrDA и др., не требующиеся для получения доступа к ГИС «РКС», должны быть отключены [ЗИС.20];

В случае необходимости скачивания информации из ГИС «РКС» на МУ по завершению сеанса работы пользователем должно проводится удаление скачанной информации или принятие иных мер, исключающих несанкционированный доступ к информации на МУ [ЗИС.30];

В отношении применяемых МУ специалистами по защите информации ведомств и (или) оператора ГИС «РКС» может быть проведена выборочная проверка соблюдения требований [ЗИС.30].

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

[1] в данном документе и далее указывается условное обозначение реализуемых организационно-технических мер по нормативным документам ФСТЭК России