Приложение №3 к приказу
от «___» _____2024 г. № ____

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

РЕГЛАМЕНТ

удалённого доступа к ресурсам локально вычислительной сети
ФГБОУ ВО СамГМУ Минздрава России

Самара 2024

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Регламент удалённого доступа к ресурсам локально вычислительной сети ФГБОУ ВО СамГМУ Минздрава России (далее – Регламент) определяет порядок доступа работников к ресурсам и сервисам локально-вычислительной сети из глобальной сети Интернет.

1.2. Регламент предназначен для применения всеми работниками, во всех структурных подразделениях, использующих средства удаленного доступа к локально-вычислительной сети.

1.3. Пересмотр настоящего Регламента происходит при изменении законодательства Российской Федерации и утверждении локальных нормативных и организационных документов, регламентирующих работу с локальными вычислительными сетями.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место удалённого доступа (АРМ УД)** – служебный персональный компьютер или ноутбук служащий для удалённого доступа к локальной сети ФГБОУ ВО СамГМУ Минздрава России.

2.2. **Информация** – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

2.3. **Авторизация**– предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

2.4. **Локальная вычислительная сеть (ЛВС)** – вычислительная сеть, охватывающая территорию ФГБОУ ВО СамГМУ Минздрава России и использующая ориентированные на эту территорию средства и методы передачи данных.

2.5. С**етевой ресурс**– устройство или часть информации, к которой может быть осуществлён удалённый доступ с другого компьютера, обычно через локальную вычислительную сеть.

2.6. **Средство криптографической защиты информации (СКЗИ)** - совокупность аппаратных и(или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении;

III. Организация удалённого доступа

3.1. Удаленный доступ сотрудника к ЛВС, предоставляет Управления информационной безопасности, в соответствии со служебной запиской руководителя структурного подразделения. В служебной записке должно быть указана ФИО сотрудника, должность, причина необходимости удалённого доступа к ЛВС, имя служебного АРМ УД и инвентарный номер.

3.2. Удалённый доступ разрешается только со служебных АРМ УД выданных согласно установленным правилам материального учета. Доступ к ЛВС осуществляется с помощью программно-аппаратного комплекса VipNet Client.

3.3. После оформления служебной записки АРМ УД предоставляется в Управления информационной безопасности для его дальнейшей настройки и установки VipNet Client.

3.4. Управления информационной безопасности производит настройку АРМ УД и уведомляет сотрудника о его получении.

3.5. При получении АРМ УД сотрудник ознакомляется с «Инструкции пользователей средств криптографической защиты информации в ФГБОУ ВО СамГМУ Минздрава России», расписывается за выдачу СКЗИ и получения пароля.

IV. Ответственность

4.1. Пользователи АРМ УД обязаны:

- осуществлять эксплуатацию СКЗИ в соответствии с документацией на СКЗИ, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области;

- не разглашать конфиденциальную информацию, к которой они, допущены;

- выполнять общие требования, предъявляемые к работе с использованием средств криптографической защиты информации и обеспечивать безопасность конфиденциальной информации, в соответствии с установленным законодательством РФ, внутренними организационно-распорядительными документами ФГБОУ ВО СамГМУ Минздрава России;

- соблюдать правила работы с СКЗИ и установленный режим разграничения доступа к техническим средствам, программам, базам данных, файлам и другим носителям конфиденциальной информации при ее обработке;

- соблюдать инструкцию по использованию персонального компьютера и ресурсов сети.

4.2 В случае утери АРМ УД или компрометации пароля сотрудник обязан сообщить об этом в Управления информационной безопасности, написать

объяснительную записку на имя Директора Института цифрового развития об утере.

V. Контроль использования удалённого доступа

5.1. Контроль действий пользователей в ЛВС осуществляют Управления информационной безопасности.

5.2. При выявлении нарушений требований информационной безопасности сотрудники Управления информационной безопасности докладывают об обнаруженных нарушениях Директору Института цифрового развития.

5.3. По фактам нарушений требований информационной безопасности, по решению Директора Института цифрового развития назначаются служебные расследования (проверки).