УТВЕРЖДАЮ

Директор ГКУ ТО ЦИТТО

_____ Усманов А.Р.

«___»_____2020г.

Государственная информационная система в сфере здравоохранения Тюменской области

Система информационной безопасности

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПРИ РАБОТЕ В ГИСЗ ТО

г.Тюмень

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция пользователя (далее — Инструкция) устанавливает правила и требования по безопасности персональных данных при их обработке в Государственной информационной системе в сфере здравоохранения Тюменской области (далее — ГИСЗ ТО).

1.2. Пользователь ГИСЗ ТО (далее — Пользователь) имеет соответствующие полномочия, установленные должностными инструкциями, трудовым договором, внутренними руководящими документами, нормативной документацией и законодательством Российской Федерации в области персональных данных, и осуществляет обработку персональных данных (далее — ПДн) в ГИСЗ ТО.

1.3. Пользователями являются работники медицинских организаций Тюменской области и других организаций, заключивших соглашение о присоединении к ГИСЗ ТО, и использующие при обработке персональных данных средства автоматизированной обработки информации ГИСЗ ТО, в том числе средства вычислительной техники, программное обеспечение, электронные носители персональных данных и средства защиты информации (далее — СЗИ), входящие в состав ГИСЗ ТО.

1.4. Пользователь несет персональную ответственность за свои действия в соответствии с нормативными актами, включая соглашение о неразглашении конфиденциальной информации (персональных данных). Действия Пользователя, нарушающие положения трудового, административного и уголовного законодательства, повлекшие нанесение серьезного ущерба субъекту(ам) персональных данных, могут повлечь дисциплинарную, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

1.5. Пользователь в своей работе руководствуется законодательством Российской Федерации в области защиты персональных данных, настоящей Инструкцией и иными нормативно-методическими документами.

1.6. Методическое руководство вопросами безопасности персональных данных в медицинских организациях осуществляется лицом, ответственным за безопасность ПДн в ГИСЗ ТО. Отдельные мероприятия по защите персональных данных проводятся структурным подразделением медицинских организаций,

назначенным лицом, сторонними организациями, привлекающимися на основании договора, ответственным за обеспечение безопасности ПДн.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ГИСЗ ТО

2.1. Пользователь ГИСЗ ТО в рамках своих должностных полномочий обязан:

2.1.1. выполнять на автоматизированном рабочем месте (далее — АРМ) только те процедуры и функции, которые определены для него правилами разграничения доступа, функциональными обязанностями и должностными инструкциями.

2.1.2. знать и выполнять требования по неавтоматизированному режиму обработки персональных данных, учету, хранению и пересылке носителей персональных данных, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.1.3. соблюдать требования внутренних нормативных документов, а также законодательства Российской Федерации в области обеспечения безопасности персональных данных.

2.1.4. располагать экран монитора АРМ в помещении, в котором происходит обработка персональных данных, во время работы так, чтобы исключалась возможность несанкционированного просмотра отображаемой на экране информации посторонних лиц, как внутри, так и вне помещения, прозрачные перегородки между помещениями при обработке персональных данных должны быть закрыты жалюзи (шторами).

2.2. Обо всех произошедших, происходящих и потенциальных нарушениях, связанных с безопасностью персональных данных в ГИСЗ ТО, пользователь должен сообщать уполномоченным лицам ответственным за безопасность ПДн в организации.

2.3. Для получения помощи по вопросам работы и настройке элементов ГИСЗ ТО пользователь должен обращаться в службу технической поддержки оператора ГИСЗ ТО или к ответственному за безопасность ПДн в организации.

2.4. Пользователям ГИСЗ ТО строго запрещается:

2.4.1. разглашать персональные данные и сведения об их защите или иным образом допускать распространение такой информации третьим лицам без санкции уполномоченных лиц;

2.4.2. копировать персональные данные на внешние материальные носители без санкции уполномоченного лица;

2.4.3. использовать для санкционированного хранения персональных данных внешние носители без соответствующей маркировки и учета;

2.4.4. допускать утерю электронных носителей персональных данных;

2.4.5. самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять аппаратное обеспечение, нарушать установленный алгоритм функционирования технических и программных средств ГИСЗ ТО или иным образом воздействовать на штатный режим работы ГИСЗ ТО и средств защиты персональных данных;

2.4.6. открывать доступ неограниченному кругу лиц к своим рабочим разделам (каталогам) на рабочей станции, входящей в состав ГИСЗ ТО;

2.4.7. несанкционированно подключать к автоматизированному рабочему месту и другим информационным ресурсам ГИСЗ ТО внешние носители, средства связи и передачи информации;

2.4.8. отключать (блокировать) временно или постоянно средства защиты информации или отдельные функции защиты АРМ ГИСЗ ТО;

2.4.9. обрабатывать на АРМ постороннюю информацию и выполнять функции, не предусмотренные должностной инструкцией, политиками, положениями и регламентами обработки персональных данных и информационной безопасности;

2.4.10. сообщать или иным образом допускать распространение посторонним лицам своих и чужих паролей, ключей, атрибутов доступа к ресурсам ГИСЗ ТО;

2.4.11. несанкционированно привлекать третьих лиц для ремонта, переконфигурирования или утилизации АРМ.

2.5. При отсутствии временного или постоянного контроля за автоматизированным рабочим местом со стороны санкционированного Пользователя доступ к компьютеру должен быть немедленно заблокирован. Для этого на АРМ с операционной системой Windows необходимо нажать одновременно комбинацию клавиш <Ctrl>+<Alt>+<Del> и выбрать опцию <Блокировка>, либо нажать комбинацию <Win>+<L>

2.6. Пользователь обязан принимать все необходимые меры по незамедлительному реагированию в случае возникновения в ходе обработки персональных данных внештатных ситуаций и чрезвычайных ситуаций, либо воздействия на средства хранения и обработки персональных данных ГИСЗ ТО разрушительных факторов, с целью ликвидации их последствий. Любые случаи нарушения безопасности должны быть незамедлительно сообщены лицу, ответственному за обеспечение безопасности ГИСЗ ТО.

2.7. Если Пользователь в штатном режиме обработки персональных данных в ГИСЗ ТО или при чрезвычайной ситуации не может выполнить в полной мере свои функции и обязанности и/или предотвратить нарушение безопасности персональных данных, он обязан заблокировать доступ к персональным данным, материальным носителям и автоматизированному рабочему месту до выяснения и устранения причин уполномоченными лицами.

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАШИТЫ

3.1. Учетные записи и пароли доступа к информационным ресурсам ГИСЗ ТО (АРМ, отдельным программам, сетевым ресурсам) предоставляются Пользователям в соответствии с регламентирующими документами ГИСЗ ТО.

3.2. Смена паролей учетных записей в ГИСЗ ТО проводится на основании заявки в установленном порядке.

3.3. Во время ввода паролей необходимо исключить возможность его подсматривания или угадывания посторонними лицами (окна, зеркала и другие отражающие поверхности) или техническими средствами (видеокамеры, программы запоминания паролей и т.п.).

3.4. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, в личном телефоне и на других носителях информации, сообщать третьим лицам личный пароль и регистрировать других лиц в системе под своим паролем, пересылать пароль любыми средствами связи (телефонная связь, электронная почта, SMS и т. п.).

3.5. При использовании паролей в ГИСЗ ТО Пользователи обязаны:

3.5.1. четко знать и строго выполнять требования настоящей инструкции и других политик и положений по безопасности персональных данных и информационной безопасности;

3.5.2. своевременно сообщать в установленном порядке лицу, ответственному за обеспечение безопасности персональных данных, об утере, компрометации, несанкционированном изменении и распространении паролей и несанкционированном изменении сроков действия паролей.

4. ПОРЯДОК РАБОТЫ В СЕТЯХ ОБЩЕГО ДОСТУПА И МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА

4.1. Работа в сетях общего доступа (Интернет) при одновременном взаимодействии с информационными ресурсами ГИСЗ ТО должна проводиться только в порядке, установленном должностными инструкциями.

4.2. При работе с сетями общего доступа Пользователю ГИСЗ ТО строго запрещается:

4.2.1. осуществлять работу с персональными данными при заблокированных средствах защиты ГИСЗ ТО (антивирус, персональный межсетевой экран и т.п.), или при отключенных отдельных функциях защиты ГИСЗ ТО;

4.2.2. передавать по открытым сетям (включая Интернет) конфиденциальные данные в нарушение установленного в ГИСЗ ТО порядка.

4.2.3. строго запрещается загружать на АРМ и подключенные к нему электронные носители информации из открытых сетей программное обеспечение, а также файлы, открытие или исполнение которых может потенциально нанести ущерб информационной безопасности (исполняемые файлы, драйверы устройств, документы с макросами, активные компоненты (plug-ins, ActiveX, Java, Flash и т. п.) браузера или ПО);

4.2.4. запрещается нецелевое использование подключения к открытым сетям вне должностных функций и с личными целями, в т.ч. сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО, сайты с экстремистским содержанием, сайты со средствами взлома или нанесения иного ущерба и т.п.).