Приложение № 17
к Положению об обработке и защите персональных данных в ОГБУ «ЦСА г. Томска»,
утвержденному приказом ОГБУ «ЦСА г. Томска» от 13.09.2021 № 102

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
администратора информационной безопасности ОГБУ «ЦСА г. Томска»

1. Общие положения.

1.1. Администратор информационной безопасности назначается нормативным актом и отвечает за обеспечение устойчивой работоспособности и информационной безопасности объекта информатизации.

1.2. Администратор информационной безопасности несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (СВТ) на объекте вычислительной техники (ОВТ) ИСПДн, а также правильность использования и нормального функционирования средств защиты информации (СЗИ), подготовку сотрудников по вопросам безопасной обработки информации на СВТ.

2. Функции администратора информационной безопасности.

2.1. Осуществляет настройку и сопровождение системы защиты от НСД на ОВТ, при этом:

реализует полномочия доступа для каждого пользователя к элементам защищаемых информационных на основе утвержденного руководством перечня лиц, допущенных к обработке защищаемой информации в ИСПДн;

вводит описание пользователей ОВТ в информационную базу системы защиты от НСД;

назначает временные пароли к информационным ресурсам и вводит в базу данных системы защиты описание полномочий доступа пользователей к защищаемым ресурсам;

своевременно удаляет описание пользователя из базы данных при увольнении или перемещении сотрудника;

периодически производит или организовывает смену паролей пользователями для доступа в систему обработки информации ОВТ.

Осуществляет настройку и сопровождение подсистемы регистрации и учета:

вводит в базу данных системы защиты от НСД описания событий, подлежащих регистрации в системном журнале;

проводит регулярный анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

своевременно информирует руководство о несанкционированных действиях персонала и организует расследование попыток НСД.

Сопровождает подсистемы обеспечения целостности рабочего программного обеспечения (ПО):

проводит периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий исполнителей ОВТ;

осуществляет восстановление системы защиты от НСД при сбоях;

проводит контроль соответствия общесистемной программной среды эталону;

обеспечивает поддержание установленного порядка и соблюдение требований

инструкции по антивирусной защите.

Участвует в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

Производит выдачу исполнителям временных паролей для средств защиты информации (СЗИ) от несанкционированного доступа (НСД), а также осуществляет оперативный контроль за действиями пользователей ОВТ.

3. Администратор информационной безопасности обязан:

3.1. Обеспечивать функционирование и поддерживать работоспособность средств защиты ИСПДн в пределах возложенных на них функций.

3.2. В случае отказа работоспособности технических средств и программного обеспечения СВТ, в том числе средств защиты АРМ принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.3. Информировать руководство о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам АРМ.

4. Администратор информационной безопасности имеет право:

4.1. Контролировать работу пользователей на автоматизированных рабочих местах АРМ.

4.2. Требовать прекращения обработки информации, как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ.