УТВЕРЖДЕНА

приказом директора
ОГБУ «КЦСО ЕАО»
от «02» 07 2024 г. № 184

ИНСТРУКЦИЯ
администратора информационной безопасности областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»

Общие положения.

Настоящая инструкция определяет общие функции, права и обязанности администратора информационной безопасности (далее – администратор ИБ) по вопросам обеспечения информационной безопасности при обработке персональных данных на автоматизированных рабочих местах (далее – АРМ), входящих в состав информационной системы персональных данных (далее – ИСПДн).

Администратор ИБ областного государственного бюджетного учреждения «Комплексный центр социального обслуживания ЕАО» (далее – Учреждение) является ответственным должностным лицом Учреждения, уполномоченным на проведение работ по технической защите информации и поддержанию уровня защиты ИСПДн, обладает правами доступа к любым программным и аппаратным ресурсам ОГБУ «КЦСО ЕАО».

Администратор ИБ назначается приказом руководителя и обеспечивает правильное использование и функционирование установленных средств защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД).

В своей работе администратор ИБ руководствуется законодательством Российской Федерации в области обеспечения безопасности персональных данных (далее – ПДн), а также организационно-распорядительными документами Учреждения.

Настоящая инструкция разработана на основании действующих нормативных документов по защите персональных данных.

1. Основные функции администратора информационной безопасности.

1.1. Администратор ИБ должен знать перечень и условия обработки персональных данных в ОГБУ «КЦСО ЕАО», перечень установленных

в кабинетах Учреждения технических средств, в том числе съёмных носителей, конфигурацию ИСПДн и перечень задач, решаемых с её использованием.

1.2. Контроль за выполнением требований, действующих нормативных и руководящих документов по защите персональных данных, при проведении работ на АРМ.

1.3. Работа с учётными записями пользователей ИСПДн (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам ИСПДн согласно разрешительной системе доступа.

1.4. Своевременная корректировка разрешительной системы доступа:

- изменение списка постоянных пользователей ИСПДн (ввод или удаление пользователя из ИСПДн);

- изменение прав доступа к защищаемым программным ресурсам или портам ввода-вывода ИСПДн.

1.5. Контроль доступа пользователей к работе на АРМ (в соответствии с перечнем должностей, замещение которых предусматривает данный доступ), выдача внешних носителей информации и соблюдения пользователями требований нормативных и руководящих документов.

1.6. Организация и проведение работ по ежегодной смене паролей пользователей для доступа к АРМ.

1.7. Сопровождение системы обеспечения целостности информации при обработке на АРМ:

- соблюдение установленных правил антивирусной защиты;

- контроль соблюдения пользователями установленных правил по информационной безопасности.

1.8. Обеспечение работоспособности ИСПДн, безопасности персональных данных, обрабатываемых, передаваемых и хранимых при помощи средств вычислительной техники в ИСПДн Учреждения.

1.9. Осуществление методического руководства и сопровождения пользователей ИСПДн по вопросам обеспечения безопасности ПДн совместно с лицом, ответственным за организацию обработки ПДн.

1.10. Администратор несёт персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе с ИСПДн, состоянием и поддержанием установленного уровня защиты ИСПДн.

2. Администратор информационной безопасности имеет право:

2.1. Осуществлять оперативный контроль за работой пользователей АРМ и адекватно реагировать на возникающие нештатные ситуации.

2.2. Требовать от специалистов Учреждения соблюдения требований

Политики информационной безопасности, нормативно-правовых актов Учреждения по информационной безопасности и исполнения настоящей инструкции.

2.3. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследования инцидентов информационной безопасности и фактов (попыток) несанкционированного доступа.

2.4. Требовать от пользователей прекращения обработки информации в ИСПДн в случае:

- нарушения установленного порядка работ;
- нарушения работоспособности средств и систем защиты информации.

3. Администратор информационной безопасности обязан:

3.1. Обеспечивать правильное функционирование и поддерживать работоспособность средств СЗИ от НСД в пределах, возложенных на него функций.

3.2. В случаях отказа СЗИ от НСД принимать меры по восстановлению их работоспособности.

3.3. Проводить инструктаж пользователей по правилам работы на АРМ.

3.4. Немедленно докладывать об инцидентах информационной безопасности руководителю ОГБУ «КЦСО ЕАО».

3.5. Вносить изменения в нормативно-правовые документы ОГБУ «КЦСО ЕАО» по информационной безопасности по необходимости.

3.6. Вводить полномочия специалистов ОГБУ «КЦСО ЕАО» в разрешительную систему доступа, обеспечивать их своевременную корректировку.

3.7. Регистрировать факты выдачи съёмных носителей информации в журнале учёта выдачи съёмных носителей.

4. Порядок пересмотра инструкции.

4.1. Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Учреждения, приводящих к существенным изменениям технологии обработки информации, с целью проверки соответствия положений данного документа реальным условиям применения. Полный пересмотр данного документа проводит ответственный за обеспечение безопасности ПДн Учреждения.

4.2. В иных случаях Инструкция подлежит частичному пересмотру. Частичный пересмотр проводит ответственный за организацию обработки ПДн. Вносимые изменения не должны противоречить другим положениям Инструкции.