Приложение 8
к приказу ГБОУ ОЦДиК
от 29.12.2017 г.№ 245

Инструкция
по работе ответственного лица за организацию обработки персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности, права и ответственность ответственного лица за организацию обработки персональных данных ГБОУ «Областной центр диагностики и консультирования» (далее – Учреждение).

1.2. Ответственное лицо за организацию обработки персональных данных является штатным работником Учреждения и назначается Приказом Директора Учреждения.

1.3. Ответственное лицо за организацию обработки персональных данных (далее - Ответственный) - лицо, отвечающее за организацию обработки персональных данных с использованием средств автоматизации и без использования таких средств.

1.4. Решение вопросов организации защиты персональных данных в Учреждении входит в прямые трудовые обязанности Ответственного.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Учреждения.

1.7. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

1.8. Ответственный обладает правами доступа к любым носителям персональных данных Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Блокирование персональных данных - временное прекращение обработки персональных данных.

2.2. Доступ к информации – возможность получения информации и ее использования.

2.3. Защита информации — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.4. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.5. Информационная система персональных данных (ИСПДн) - совокупность

содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.6. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.7. Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

2.8. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.9. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.10. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.11. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

3.1. В области автоматизированной обработки персональных данных Ответственный обязан:

3.1.1. взаимодействовать с администратором безопасности и ответственным за обеспечение безопасности персональных данных по вопросам обеспечения и выполнения требований обработки персональных данных;

3.1.2. контролировать осуществление мероприятий по установке и настройке средств защиты;

3.1.3. осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных носителей, содержащих персональные данные.

3.2. В области обработки персональных данных без использования средств автоматизации Ответственный обязан:

3.2.1. контролировать порядок обработки бумажных носителей персональных данных;

3.2.2. осуществлять проверки наличия документов, содержащих персональные данные.

3.3. В области информирования работников Ответственный обязан:

3.3.1. доводить до сведения работников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3.3.2. осуществлять методическое руководство работников, имеющих санкционированный доступ к персональным данным, в вопросах обеспечения безопасности персональных данных;

3.3.3. организовывать повышение квалификации работников в области защиты персональных данных.

3.4. В области работы с субъектами персональных данных Ответственный обязан:

3.4.1. разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных;

3.4.2. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3.5. В области контроля работников Ответственный обязан:

3.5.1. планировать мероприятия по организации обеспечения безопасности персональных данных;

3.5.2. организовывать и осуществлять периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;

3.5.3. организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

3.6. В области учета лиц, имеющих доступ к персональным данным, Ответственный обязан:

3.6.1. знать и предоставлять на утверждение Директору Учреждения изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей;

3.6.2. участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

3.7. Иные обязанности Ответственного:

3.7.1. по указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по правилам обработки персональных данных;

3.7.2. знать перечень и условия обработки персональных данных в Учреждении;

3.7.3. осуществлять организацию учёта документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

3.7.4. выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. ПРАВА ОТВЕТСТВЕННОГО

Ответственный имеет право:

4.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки и обеспечения безопасности персональных данных.

4.2. Требовать от всех пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

4.3. Инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

4.4. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

4.5. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

4.6. Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

4.7. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

5. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

5.2.2. доложить Директору Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за обеспечение безопасности персональных данных и администратора безопасности о факте несанкционированного доступа.

6. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции;

6.1.2. правильность и объективность принимаемых решений;

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных;

6.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.