Министерство здравоохранения Омской области

Бюджетное учреждение здравоохранения Омской области

«КЛИНИЧЕСКИЙ ДИАГНОСТИЧЕСКИЙ ЦЕНТР»

(БУЗОО «КДЦ»)

ПРИКАЗ

10 апреля 2017 г. № 23

г. Омск

Об организации работы с персональными данными

В целях соблюдения требований Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 18 февраля 2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Федерального закона от 21 ноября 2011г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и других нормативно-правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных БУЗОО «КДЦ»,

п р и к а з ы в а ю:

1. Назначить заместителя Главного врача по организационно-методической работе Бодрову Т.В. Ответственным за организацию обработки персональных данных в БУЗОО «КДЦ».

2. Назначить ведущего специалиста по защите информации отдела автоматизированных систем управления администратором информационной безопасности, ответственным за антивирусную проверку и за разработку, проведение мероприятий, направленных на выполнение требований законодательства и других нормативных документов в области персональных

данных, в его отсутствие эти обязанности возлагать на ведущего программиста отдела автоматизированных систем управления.

3. Утвердить:

3.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных БУЗОО "КДЦ" (Приложение 1).

3.2. Порядок удаления (изменения) персонифицированных записей из (в) информационных системах персональных данных БУЗОО "КДЦ" (Приложение 2).

3.3. Форму Акта об удалении (уничтожении) персонифицированных записей из информационных систем персональных данных (Приложение 3).

3.4. Форму отметки об исполнении заявлений от субъектов персональных данных (Приложение 4).

3.5. Форму Журнала регистрации обращений субъектов персональных данных на предоставление доступа к своим персональным данным (Приложение 5).

3.6. Состав комиссии по установлению уровней защищенности информационных систем персональных данных и по уничтожению носителей персональных данных (Приложение 6).

3.7. Форму Заявления о согласии на обработку персональных данных работника БУЗОО «КДЦ» (Приложение 7).

3.8. Форму Согласия на обработку персональных данных (Приложение 8).

3.9. Порядок выявления инцидентов информационной безопасности информационных систем персональных данных (Приложение 9).

3.10. Форму карточки данных об инциденте информационной безопасности (Приложение 10).

4. Комиссии по установлению уровней защищенности информационных систем персональных данных в срок до 23.07.2017 г. провести мероприятия по установлению уровней защищенности информационных систем персональных данных с составлением и утверждением соответствующих актов.

5. Начальнику кадрово–правовой службы Ягодке А.М. внести соответствующие изменения в должностную инструкцию заместителя Главного врача по организационно-методической работе Бодровой Т.В., начальнику отдела АСУ Юсупову Р.Х. внести соответствующие изменения в должностные инструкции ведущего специалиста по защите информации отдела автоматизированных систем управления Бажанова В.С и ведущего программиста отдела автоматизированных систем управления Иванова С.В. в срок до 1.07.2017г.

6. Настоящий приказ вступает в силу с момента его подписания.

7. Контроль за исполнением Приказа оставляю за собой

Главный врач Н.И. Орлова

Р.Х Юсупов

2-68

Приложение 1
к Приказу
от 10.04.2017 № 23

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных БУЗОО "КДЦ"

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных БУЗОО «КДЦ» (далее – «Положение») разработано во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, Федерального закона от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников», Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и других нормативно-правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Настоящее положение определяет политику БУЗОО «КДЦ» (далее – Оператор) в отношении обработки персональных данных и является общедоступным документом.

1.3. Требования настоящего Положения являются обязательными для исполнения всеми работниками Оператора, получившими доступ к персональным данным.

1.4. Решения об изменении настоящего Положения принимаются на основании:

– результатов проведенных аудитов, мероприятий по контролю и надзору за обеспечением безопасности персональных данных, осуществляемых уполномоченными органами;

– изменений нормативно-правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн);

– изменений процессов обработки персональных данных в информационных

– системах персональных данных Оператора;

– результатов анализа инцидентов информационной безопасности в ИС персональных данных.

1.5. В настоящем Положении используются следующие понятия и термины:

– **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

– **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;

– **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

– **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

– **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

– **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;

– **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

– **трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти

иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.6. Оператором является:

Наименование Оператора: Бюджетное учреждение здравоохранения Омской области "Клинический диагностический центр"

ИНН: 5504001891

Адрес местонахождения: 644024, Омская обл., г. Омск, ул. Ильинская, д. 9;

644015, Омская обл., г. Омск, ул. Суворова, д. 112.

1.7. Обработка персональных данных осуществляется с 01.01.1992 на основании включения в реестр Операторов, осуществляющих обработку персональных данных (Регистрационный номер 09-0039483 от 27.02.2009).

2. Общие принципы и условия обработки персональных данных

2.1. Оператор осуществляет обработку персональных данных работников и лиц, не являющихся таковыми.

2.2. Обработка осуществляется в целях исполнения функций, определенных законами и иными нормативно-правовыми актами Российской Федерации, а также в рамках осуществления видов деятельности, определенных во внутренних документах Оператора.

2.3. При обработке персональных данных Оператор руководствуется следующими принципами и условиями:

– обработка персональных данных должна осуществляться на законной и справедливой основе;

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных за исключением случаев, определенных пп. 2-11 ч.1 ст. 6 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных»;

– обработка специальных категорий персональных данных осуществляется в случаях, предусмотренных пп.1-10 ч.2. ст. 10 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных»;

– обработка биометрических категорий персональных данных осуществляется только при наличии согласия в письменной форме субъекта персональных данных за исключением случаев, предусмотренных ч.2. ст. 11 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных»;

– Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение Оператора). Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом. В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена

обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных»;

– обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

– при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

– хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

2.4. Оператор самостоятельно определяет содержание, объем, цели обработки и сроки хранения персональных данных.

2.5. Принятые Оператором документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений доводятся до работников Оператора в части касающихся их.

3. Цели обработки персональных данных

3.1. Обработка персональных данных осуществляется:

- в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

- для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

4. Категории обрабатываемых персональных данных, источники их получения, сроки обработки и хранения

4.1. В информационных системах персональных данных Оператора обрабатываются следующие категории персональных данных:

– Персональные данные работников;

– Персональные данные пациентов, в том числе касающиеся состоянии здоровья.

4.2. Обработка персональных данных прекращается при достижении целей обработки, утрате правовых оснований обработки, окончании сроков хранения документов.

5. Сведения о третьих лицах, участвующих в обработке персональных данных

5.1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки Оператор, а также с согласия субъектов персональных данных в ходе своей деятельности предоставляет персональные данные следующим организациям:

– При получении, в рамках установленных полномочий, мотивированных запросов органам прокуратуры, правоохранительным органам, органам безопасности, государственным инспекторам труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченным запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

5.2. Оператор не поручает обработку персональных данных другим лицам.

6. Обязанности и права Оператора персональных данных

6.1. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных.

6.2. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

6.3. Оператор обязан рассмотреть возражение, против решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

6.4. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную ч.7 ст. 14 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных».

6.5. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

6.6. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

6.7. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.8. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

6.9. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных

персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.10. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.11. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.12. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных» или другими

нормативно-правовыми актами.

6.13. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

6.14. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п. 7.11-7.13 настоящего положения, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7. Права субъектов персональных данных

7.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.

7.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.3. В случае, если сведения, указанные в ч. 7 ст. 14 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных», а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо

выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.4. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в ч. 7 ст. 14 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в ч. 4 ст. 14 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

7.5. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» в следующих случаях:

– если обработка персональных данных, включая те, что получены в результате оперативно–розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях укрепления обороны страны, обеспечения безопасности государства и охраны правопорядка;

– если обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

– если обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

– если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

– если обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

– если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8. Меры по обеспечению безопасности персональных данных при их обработке

8.1. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

8.2. Обеспечение безопасности достигается:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

9. Ответственность за разглашение информации, связанной с персональными данными

9.1. Лица, виновные в нарушении требований настоящего Положения, несут ответственность, предусмотренную законодательством Российской Федерации.

9.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Положением и Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Положением и Федеральным законом, подлежит возмещению в

соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложение 2
к Приказу
от 10.04.2017 № 23

ПОРЯДОК
удаления (изменения) персонифицированных записей из (в) информационных систем персональных данных
БУЗОО "КДЦ"

1. Перечень используемых определений, обозначений и сокращений

АИБ –администратор информационной безопасности.
ИС – информационная система.
ИСПДн – информационная система персональных данных.
КИ – конфиденциальная информация.
НЖМД – накопитель на жёстких магнитных дисках.
ПДн – персональные данные.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

2. Общие положения

2.1. Настоящая Инструкция устанавливает основные требования к удалению (изменению) персонифицированных записей из (в) ИСПДн БУЗОО "КДЦ.

2.2. Ответственность за соблюдение требований настоящей инструкции работниками БУЗОО "КДЦ" возлагается персонально на работников, контроль – возлагается на АИБа.

2.3. Положения данной инструкции обязательны для выполнения всеми работниками БУЗОО "КДЦ", обрабатывающими ПДн в ИСПДн БУЗОО "КДЦ", а также имеющими допуск к обработке ПДн.

2.4. Полное (частичное) удаление персонифицированных записей о субъектах ПДн производится по достижении цели обработки таких данных, указанных в согласии на обработку или по письменному заявлению субъекта ПДн о прекращении обработки его ПДн (заявления о сокращении перечня ПДн, предъявляемых для обработки). Полное (частичное) удаление персонифицированных записей производится в течение 3 дней с момента подачи заявления от субъекта ПДн.

2.5. Изменение ПДн субъекта производиться только по его письменному заявлению об уточнении обрабатываемых ПДн в течение 3 дней с момента подачи заявления.

3. Порядок удаления (изменения) персонифицированных записей из (в) информационных систем персональных данных

3.1. Уничтожение ПДн из ИСПДн производится средствами ИСПДн, предусматривающими выполнение данной операции.

3.2. По факту полного/частичного удаления персонифицированных записей комиссией из 3-х человек, в состав которой должен входить работник, работающий с ИСПДн, составляется Акт. По факту уничтожения ПДн из нескольких ИСПДн допускается оформлять один Акт. Акт хранится у АИБа в течение 3 лет.

3.3. В случае если удаление ПДн производиться по заявлению субъекта о прекращении обработки его ПДн (о сокращении перечня ПДн, предъявляемых для обработки), по факту исполнения заявления работником БУЗОО "КДЦ", выполнившим удаление ПДн, на заявлении делается дополнительная отметка об исполнении. Примечание: Данных пункт не отменяет требования п. 3.2 настоящего порядка.

3.4. По факту изменения ПДн, производящегося по заявлению субъекта об уточнении обрабатываемых его ПДн, работником БУЗОО "КДЦ", выполнившим данные изменения, на заявлении делается отметка об исполнении.

Приложение 3
к Приказу
от 10.09.2017 № 23

ФОРМА

Акта об удалении (уничтожении) персонифицированных записей из информационных систем персональных данных

Акт №__
об удалении (уничтожении) персонифицированных записей из информационных систем персональных данных

Дата г Омск

Комиссия в составе:

Председатель:

– Орлова Наталья Ивановна - Главный врач

Члены комиссии:

- Бодрова Татьяна Валентиновна – Заместитель главного врача по организационно-методической работе;
- Ягодка Алла Михайловна – Начальник кадрово-правовой службы;
- Юсупов Рустам Хасанович – Начальник отдела АСУ;
- Примаков Александр Владиславович – Ведущий юрисконсульт.

составила настоящий Акт о том, что в ее присутствии уничтожены следующие персонифицированные записи о субъектах персональных данных из следующих информационных систем персональных данных:

1. ИСПДн «_____»:

название ИСПДн

ФИО субъекта	Номер документа удостоверяющего личность субъекта ПДн (при необходимости)	Категория субъекта ПДн	Категория обрабатываемых ПДн субъекта: перечень заполненных полей ИСПДн	Причина удаления	Способ уничтожения (форматирование, с использованием специальных программных средств (каких))
1	2	3	4	5	6

2. ИСПДн «_____»:

название ИСПДн

Председатель комиссии:	Орлова Н.И.
Члены комиссии:	Бодрова Т.В. Ягодка А.М. Юсупов Р.Х. Примаков А.В.

Настоящий Акт составлен в 1-ом экземпляре на ___ листах каждых.
Экз. №1 – Администратор информационной безопасности.

Приложение 4
к Приказу
от 10.04.2017 № 23

ФОРМА
отметки об исполнении заявлений от субъектов персональных данных

ОТМЕТКА
об исполнении заявлений от субъектов персональных данных

Исполнено

ФИО исполнителя:_____

Должность исполнителя:_____

Название ИСПДн, в которых вносились данные изменения (уточнение, удаление):_____

Дата исполнения: «_____»_____ 201_ г. /_____
подпись

Приложение 5
к Приказу
от 10.09.2018 № 23

ФОРМА
Журнала регистрации обращений субъектов персональных данных на предоставление доступа к своим персональным данным в БУЗОО "КДЦ"

Начат «____» _____ 201_ г.
Окончен «____» _____ 201_ г.
На _____ листах

№ п/п	Дата предоставления доступа	ФИО субъекта персональных данных (его законного представителя)	Номер основного документа, удостоверяющего личность субъекта персональных данных (его законного представителя), сведения о дате выдачи указанного документа и выдавшем его органе	№ и дата запроса (письма)	Форма предоставления запрашиваемой информации	ФИО, должность лица, предоставившего запрошенную информацию	Подпись субъекта персональных данных (его законного представителя)	Подпись лица, предоставившего информацию по запросу	Примечание *(с выносом, без выноса и т.д.)*
1	2	3	4	5	6	7	8	9	10

Приложение 6
к Приказу
от 10.04.2017 № 23

СОСТАВ
комиссии по установлению уровней защищенности информационных систем персональных данных БУЗОО "КДЦ" и по уничтожению материальных и электронных носителей персональных данных.

Для определения уровня защищенности информационных систем персональных данных БУЗОО "КДЦ" и для уничтожения носителей персональных данных назначается комиссия в составе:

Председатель комиссии:

– Орлова Наталья Ивановна – Главный врач.

Члены комиссии:

– Бодрова Татьяна Валентиновна – Заместитель главного врача по организационно-методической работе;

– Ягодка Алла Михайловна – Начальник кадрово-правовой службы;

– Юсупов Рустам Хасанович – Начальник отдела АСУ;

– Примаков Александр Владиславович – Ведущий юрисконсульт.

По результатам работ комиссия предоставляет Главному врачу БУЗОО "КДЦ" для утверждения Акт установления уровня защищенности информационной системы персональных данных (для каждой информационной системы персональных данных составляется отдельный акт) БУЗОО "КДЦ" либо Акт об уничтожении материальных или электронных носителей персональных данных.

Приложение 7
к Приказу
от 10.09.2017 № 23

ФОРМА
Заявления о согласии на обработку персональных данных работника БУЗОО «КДЦ»

ЗАЯВЛЕНИЕ
О согласии на обработку персональных данных

Я, _____
(Фамилия, имя, отчество)

проживающий (ая) по адресу _____
(Индекс, область, район, населённый пункт, улица, дом, корпус, квартира)

_____

Документ удостоверяющий личность: _____
(Наименование, серия и номер)

_____

_____
(Дата выдачи, организация выдавшая документ)

В соответствии с требованиями статьи 9 Федерального закона Российской Федерации от 27 июля 2006г. № 152-ФЗ «О персональных данных», даю добровольное согласие на обработку моих персональных данных БУЗОО "КДЦ", находящемуся по адресу – 644024, Омская обл., г Омск, ул. Ильинская, д. 9 (далее – «Оператор»), с целью осуществления трудовых отношений с Оператором, взаимоотношений с ИФНС, Управлением ПФР, ФСС и другими организациями для предоставления мне и членам моей семьи мер социальной поддержки.

Согласие дается Оператору для обработки следующих персональных данных: фамилия, имя, отчество, пол, дата и место рождения, адрес регистрации, и места фактического проживания, контактный телефон, реквизиты полисов обязательного и добровольного медицинского страхования, страховой номер индивидуального лицевого счета в Пенсионном фонде РФ (СНИЛС), индивидуальный номер налогоплательщика, паспортные данные (серия, номер, кем и когда выдан), сведения о воинском учете, семейное положение и состав семьи, сведения об образовании и трудовом стаже, о заработной плате, подоходном налоге, взносах в пенсионный фонд, социальных льготах, содержание трудового договора.

Предоставляю Оператору право осуществлять действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение) использование, обезличивание, блокирование персональных данных.

Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронные базы данных, включения в списки (реестры) и отчетные формы.

Я не возражаю против обмена (прием, передача) моими персональными данными между Оператором и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов, а также для осуществления мер социальной защиты.

Я не возражаю против размещения на официальном сайте учреждения моих данных (ФИО, должность, сведения из документа об образовании, сведения из сертификата специалиста, график работы и часы приёма).

Срок хранения моих персональных данных в электронных базах данных, банках данных или хранилищах данных соответствует сроку хранения приказов по личному составу учреждения (организации) и составляет 75 (семьдесят пять) лет.

Настоящее согласие действует в течении всего срока моих трудовых отношений с БУЗОО «КДЦ».

Настоящее согласие вступает в законную силу в день его подписания.

Настоящее заявление может быть отозвано мною в письменной форме в любое время по моему усмотрению.

Я осознаю, что в случае отзыва мной согласия дальнейшая обработка персональных данных Оператором будет продолжаться в целях исполнения обязательств по Трудовому договору и в соответствии с Трудовым кодексом РФ. Я ознакомлен с тем, что для полного прекращения обработки моих персональных данных Оператором должен быть, расторгнут Трудовой договор, после чего эти данные будут храниться в течение срока, определенного в соответствии с Архивным законодательством РФ.

"____" _____ 201_ г. _____/_____
дата подпись заявителя

Приложение 8
к Приказу
от 10.04.2017 № 23

ФОРМА
Согласия на обработку персональных данных

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, нижеподписавшийся _____
(Ф.И.О. полностью, дата рождения)

_____,

проживающий по адресу _____
(место регистрации)

_____

паспорт _____
(серия и номер, дата выдачи, наименование выдавшего органа)

_____

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. «О персональных данных» N 152-ФЗ подтверждаю **свое согласие** на обработку бюджетным учреждением здравоохранения Омской области «Клинический диагностический центр» (далее – Оператор) моих персональных данных, включающих: **фамилию, имя, отчество, пол, дату рождения, адрес проживания, контактный телефон, реквизиты полиса ОМС (ДМС), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью,** в медико-профилактических целях, в целях установления медицинского диагноза и **оказания медицинских услуг** при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, передачу, обезличивание, блокирование, уничтожение.

Настоящее согласие дано мной _____ и действует бессрочно.
(дата)

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи.

Почтовый адрес и контактный телефон(ы) _____

_____

Подпись субъекта персональных данных _____

Приложение 9
к Приказу
от 10.04.2017 № 23

ПОРЯДОК
выявления инцидентов информационной безопасности информационных систем персональных данных
БУЗОО "КДЦ"

1. Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.
ИБ – информационная безопасности.
ИС – информационная система.
ИСПДн – информационная система персональных данных.

2. Общие положения

2.1. Настоящий Порядок устанавливает правила выявления фактов несоблюдения условий обработки защищаемой информации, использования средств защиты информации, которые могут привести к нарушению конфиденциальности, целостности и доступности защищаемой информации данных или другим нарушениям, приводящим к снижению класса защищенности государственной информационной системы, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления и предотвращения иных инцидентов информационной безопасности ИСПДн БУЗОО "КДЦ".

2.2. Порядок разработан в соответствии с:

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– приказом от 18.02.2013 ФСТЭК № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами, а также в соответствии с локальными нормативными актами организации.

2.3. Настоящий Порядок обязателен к соблюдению всеми пользователями ИСПДн БУЗОО "КДЦ".

2.4. Разбирательство по всем инцидентам ИБ проводится администратором информационной безопасности БУЗОО "КДЦ".

3. Выявление инцидента информационной безопасности

3.1. Основными источниками информации об Инцидентах ИБ являются:

– факты, выявленные пользователями ИСПДн, администратором информационной системы, администратором информационной безопасности;

– результаты работы средств мониторинга ИБ результаты проверок и аудита (внутреннего или внешнего);

– запросы и предписания органов надзора;

– другие источники информации.

3.2. Пользователь ИСПДн может выявить признаки наличия Инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия требованиям, утвержденных в локальных актах БУЗОО "КДЦ". Любые сведения о Происшествие или Инциденте ИБ должны быть незамедлительно переданы выявившим их пользователем АИБу.

4. Анализ исходной информации и принятие решения о проведении разбирательства

4.1. АИБ после получения информации о предполагаемом Инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа работник проводит проверку наличия в выявленном факте нарушений.

4.2. По решению АИБа единичный Инцидент ИБ, не приведший к негативным последствиям и совершенный пользователем ИСПДн впервые, фиксируется в карточке данных «Инциденты ИБ» с присвоением статуса «Разбирательство не требуется».

4.3. В случае наличия признаков Инцидента ИБ, АИБ по общим вопросам определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует руководителя структурного подразделения (начальника отдела) об Инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

4.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, АИБ определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

5. Разбирательство инцидента информационной безопасности

5.1. Цели и этапы разбирательства Инцидента ИБ:

Целями разбирательства инцидентов ИБ являются:

– выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

– защита прав пользователей ИСПДн БУЗОО "КДЦ", установленных законодательством Российской Федерации;

– обеспечение безопасности защищаемой информации данных;

– предотвращение несанкционированного доступа к защищаемой информации.

Разбирательство Инцидента ИБ, состоит из следующих этапов:

– подтверждение/опровержение факта возникновения Инцидента ИБ;

– подтверждение/корректировка уровня значимости Инцидента ИБ;

– уточнение дополнительных обстоятельств (деталей) Инцидента ИБ;

– получение (сбор) доказательств возникновения Инцидента ИБ, обеспечение их сохранности и целостности;

– минимизация последствий Инцидента ИБ;

– информирование и консультирование пользователей ИСПДн по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;

– разработка мероприятий по обнаружению и/или предупреждению инцидентов ИБ.

5.2. Создание Рабочей группы для проведения расследования Инцидента ИБ:

5.3. При необходимости АИБ незамедлительно уведомляет БУЗОО "КДЦ" о факте Инцидента ИБ и инициирует создание Рабочей группы для разбирательства указанного Инцидента ИБ. Взаимодействие между членами Рабочей группы осуществляется в рабочем порядке с соблюдением при этом требований конфиденциальности. При необходимости проводятся заседания Рабочей группы, время, место и темы которых определяются ее Руководителем. В иных случаях, АИБ может проводить расследование Инцидента ИБ самостоятельно с подготовкой всех необходимых документов.

5.4. Порядок проведения разбирательства Инцидента ИБ:

В процессе проведения разбирательства Инцидента ИБ обязательными для установления являются:

– дата и время совершения Инцидента ИБ;

– ФИО, должность и подразделение Нарушителя ИБ[1];

– уровень критичности Инцидента ИБ;

– обстоятельства и мотивы совершения Инцидента ИБ;

– информационные ресурсы, затронутые Инцидентом ИБ;

– характер и размер реального и потенциального ущерба;

– обстоятельства, способствовавшие совершению Инцидента ИБ.

После получения необходимой информации по Инциденту ИБ осуществляющий разбирательство работник проводит анализ полученных данных.

Осуществляющий разбирательство работник проводит оценку негативных последствий от реализации Инцидента ИБ. В ходе данной оценки учитываются:

– прямой финансовый ущерб;

– репутационный ущерб;

---

1 В случае внутреннего нарушителя ИБ

– потенциальный ущерб;

– косвенные потери, связанные с недоступностью сервисов, потерей информации;

– другие виды ущерба или аспекты негативных последствий для БУЗОО "КДЦ" или ее пользователей.

В течение 5 (пяти) рабочих дней с момента назначения осуществляющего разбирательство работника (формирования Рабочей группы), осуществляющий разбирательство работник запрашивает у руководителя структурного подразделения (начальника отдела) объяснительную записку Нарушителя ИБ[2][2]. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение (двух) рабочих дней и представлена его непосредственным руководителем осуществляющему разбирательство работнику в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить объяснительную записку, осуществляющему разбирательство работнику предоставляется акт, составленный в соответствии с установленным порядком.

С целью минимизации последствий Инцидента ИБ возможно временное отключение прав доступа работника к Информационным системам (ИС) на время проведения расследования предварительно сделав заявку. Подобное отключение инициируется осуществляющим разбирательство работником с обязательным предварительным устным согласованием с руководителем Нарушителя.

В случае, если у Нарушителя ИБ были отключены права доступа к ИС на время проведения разбирательства, то по его результатам осуществляющий разбирательство работник по согласованию с руководителем Нарушителя ИБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у Нарушителя ИБ прав доступа к ИС либо инициирует официальную процедуру отмены (изменения) прав доступа к ИС в соответствии с установленным порядком в БУЗОО "КДЦ". Если Нарушение ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с информационными ресурсами высокого уровня безопасности, то основанием для возврата прав доступа является успешное прохождение повторного инструктажа работниками отделов, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами БУЗОО "КДЦ".

Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИС (разблокировка пользователя) может производиться только по заявке руководителя Нарушителя ИБ или осуществляющего разбирательство работника.

6. Оформление результатов проведенного разбирательства

6.1. Собранная в процессе разбирательства Инцидента ИБ информация фиксируется осуществляющим разбирательство работником в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по Инциденту ИБ.

---

2 В случае внутреннего нарушителя ИБ

6.2. Осуществляющий разбирательство работник формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию Инцидента ИБ.

6.3. Итоговое заключение по Инциденту ИБ осуществляющий разбирательство работник направляет Главному врачу БУЗОО "КДЦ".

6.4. Осуществляющий разбирательство работник фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

6.5. Осуществляющий разбирательство работник, при необходимости определения правовой оценки Инцидента ИБ, может обратиться за консультациями в другие подразделения БУЗОО "КДЦ" и соответствующие организации. В этом случае информацию по инциденту ИБ осуществляющий разбирательство работник передает с грифом «Конфиденциально».

6.6. В случае выявления в инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, осуществляющий разбирательство работник передает все материалы по Инциденту ИБ Главному врачу БУЗОО "КДЦ" для принятия решения, в соответствии с установленным порядком, о подаче заявления в правоохранительные органы Российской Федерации.

6.7. Осуществляющий разбирательство работник фиксирует полученную дополнительную информацию в карточке данных «Инциденты ИБ» и информирует Главного врача БУЗОО "КДЦ".

7. Завершение разбирательства, превентивные мероприятия

7.1. По завершению разбирательства Инцидента ИБ, осуществляющий разбирательство работник передает имеющиеся материалы (в объеме, достаточном для принятия решения) вышестоящему руководителю Нарушителя ИБ[3] для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

7.2. На основании полученных результатов разбирательства специальная комиссия в срок не более 3 (трех) рабочих дней даёт поручение руководителю структурного подразделения организовывать проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

– повторное ознакомление Нарушителя ИБ с Правилами;

– анализ и пересмотр имеющихся прав доступа к информационным ресурсам у Нарушителя ИБ;

– доведение до всех пользователей ИСПДн требований внутренних нормативных документов БУЗОО "КДЦ";

– отмена неактуальных прав доступа к информационным ресурсам;

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам,

не имеющим права доступа к такой информации;

– и другие обоснованные мероприятия.

8. Права, обязанности и ответственность участников разбирательства

8.1. Осуществляющий разбирательство работник имеет право:

– по согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам Инцидента ИБ у Нарушителя ИБ;

– запрашивать и получать от пользователей ИСПДн, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента ИБ;

– инициировать на основании заявок отключение от информационных ресурсов пользователей ИСПДн, нарушивших правила или требования ИБ, на период проведений расследования Инцидента ИБ в случае если имеется существенный риск того, что продолжение пользователя с ИС может повлечь значительное увеличение ущерба или новые инциденты ИБ;

– инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной/ материальной ответственности.

8.2. Осуществляющий разбирательство работник обязан:

– объективно и основательно проводить разбирательство каждого инцидента ИБ;

– определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;

– фиксировать в карточке данных «Инциденты ИБ» всю исходную информацию об инциденте ИБ и результаты его расследования;

– предоставлять отчеты и рекомендации по проведенным разбирательствам специальной комиссии;

– проводить анализ обстоятельств, способствовавших совершению каждого инцидента ИБ, и на его основе, разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных Инцидентов ИБ и минимизации возможности их повторения в будущем;

– составление заключений по фактам инцидентов ИБ, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

8.3. Пользователи ИСПДн обязаны:

– предоставлять по запросам проводящего разбирательство работника устные и письменные разъяснения и иную информацию в рамках своей компетенции,

– необходимую для проведения разбирательства Инцидента ИБ;

– информировать АИБа о выявленных Инцидентах ИБ.

Приложение 10
к Приказу
от 10.04.2017 № 23

ФОРМА
Карточки данных об инциденте информационной безопасности

Карточка
данных об инциденте информационной безопасности

Дата события: _____
Номер события: _____

Информация о сообщающем лице

ФИО Сообщающего: _____
Должность: _____
Организация (если сообщающее лицо состоит в сторонней организации): _____
Телефон: _____

Описание события ИБ

_____
_____
_____

Пораженные активы

Пораженные активы (если таковые имеются)
Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности
Информация/Данные: _____
Оборудование: _____
Программное обеспечение: _____
Средства связи: _____
Документация: _____

Разрешение инцидента

Дата начала расследования инцидента: _____
Фамилия лица, проводившего расследование инцидента: _____
Дата окончания инцидента: _____
Дата окончания воздействия: _____
Дата завершения расследования инцидента: _____

Заключение

Необходимо поставить отметку о том, является ли инцидент значительным или нет и добавить в краткое пояснение для обоснования этого заключения	Значительный ☐	Незначительный ☐

Пояснения:

_____

_____

_____