КРАЕВОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«АЛТАЙСКИЙ КРАЕВОЙ ЦЕНТР ПО ПРОФИЛАКТИКЕ И БОРЬБЕ СО СПИДОМ И ИНФЕКЦИОННЫМИ ЗАБОЛЕВАНИЯМИ»

П Р И К А З

27 мая 2015г. № 35

г. Барнаул

«Об организации работы по защите
конфиденциальной информации»

С целью исключения или существенного затруднения несанкционированного доступа (НСД) к конфиденциальной информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информации

ПРИКАЗЫВАЮ:

1. Утвердить:
   1.1. Положение о защите персональных данных работников (Приложение 1);
   1.2. Акт классификации информационных систем персональных данных (ИСПДн) (Приложение 2);
   1.3. Должностные обязанности администратора информационной безопасности (Приложение 4);
   1.4. Инструкцию по проведению антивирусного контроля (Приложение 6);
   1.5. Инструкцию по организации парольной защиты в АС (Приложение 7);
   1.6. Должностные обязанности программиста (Приложение 8);
   1.7. Инструкцию о порядке еженедельного технического обслуживания (ТО) персонального компьютера для пользователя (Приложение 9);
   1.8. Перечень защищаемых информационных ресурсов (Приложение 10);
   1.9. План размещения АРМ, осуществляющих обработку персональных данных (Приложение 11);
   1.10.Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (Приложение 12);
   1.11.Форму журнала учёта мероприятий по контролю за исполнением правил обработки персональных данных (Приложение 13);
   1.12.Форму журнала учёта организационно-распорядительных документов по обработке персональных данных. (Приложение 14);
   1.13.Специальную инструкцию пользователя (Приложение 15);
   1.14.Форму журнала регистрации запросов на предоставление доступа к персональным данным; (Приложение 16);

1.15.Перечень помещений, производящих обработку персональных данных (Приложение 17);

1.16.Перечень помещений, с ограничением доступа лиц, не имеющих отношения к работе с персональными данными (Приложение 18);

1.17.Форму журнала учета мероприятий по контролю за исполнением правил обработки персональных данных. (Приложение 19);

1.18.Перечень сведений ограниченного распространения; (Приложение 21);

2. Возложить:
   2.1. Персональную ответственность за сотрудниками, непосредственно осуществляющими получение данных регионального сегмента и выполняющих работу с ними за обеспечение сохранности, конфиденциальности и безопасности в ходе обработки персональных данных (Приложение 3);
   2.2. Обязанности администратора информационной безопасности на сотрудников (Приложение 5);
   2.3. Работы по установлению разграничений прав доступа пользователей на компьютеры, выдачу паролей (ключей), обучение пользователей правилам работы и обязанности по организации парольной защиты на сотрудников, ответственных за организацию эксплуатации вычислительной техники в данном учреждении (Приложение 3);
3. Закрепить:
   3.1. Компьютеры за ответственными лицами для обработки данных регионального сегмента (Приложение 20);
4. Зам. главного врача по АХЧ- Выходцеву С.Н.:
   4.1. Обеспечить физическую и техническую охрану ВП (надёжные двери, замки, решётки на окнах, сигнализация). Сдачу/приём ключей от ВП производить лицам, работающим в нём или ответственным за это помещение под роспись в журнале на вахте или у дежурного по учреждению;
5. Зам. главного врача по организационно-методической работе- Хаустовой Л.В.:
   5.1. Организовать работу с конфиденциальной информацией в структурных подразделениях в соответствии с утвержденными Перечнем и Инструкцией. (Приложение 22);
6. Контроль за исполнением приказа оставляю за собой.

Главный врач Л.В.Султанов

Приложение 1

Положение о защите персональных данных работников

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации»

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом главного врача и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:
- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

3.2.4. Персональные данные следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

3.2.6. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- бухгалтерии;
- сотрудники службы управления персоналом;
- сотрудники компьютерных отделов.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе

использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника его представителю в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключитель-

но в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным сотрудника имеют:

- главный врач учреждения;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам работник, носитель данных.
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом главного врача учреждения.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

5. Защита персональных данных

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать

неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. «Внутренняя защита».

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.5.2. Для обеспечении внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главному врачу, работникам отдела персонала и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного подразделения. (например, при подготовке материалов для аттестации работника).

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается руководителю службы управления персоналом и руководителю службы информационных технологий

5.6. «Внешняя защита».

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных.
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.4. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.

- своевременно сообщать работодателю об изменении своих персональных данных

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Приложение 2

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом
и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему **АИС «Кадры здравоохранения»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес места жительства, адрес по регистрации, вид документа, удостоверяющего личность, серия и номер этого документа, наименование или код органа, выдавшего документ, дата выдачи документа, данные об образовании, стаже работы, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до 1000 записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС

ЛПУ
Табельный номер
ФИО
Должность
Федеральный регистр
Совмещаемая должность
Дата рождения
Пол
Гражданство
Место рождения
Адрес места жительства
Семейное положение
Дата включения в регистр
Дата исключения из регистра
СНИЛС
ИНН
Тип документа, удостоверяющего личность, Серия и номер документа
Дата регистрации по месту жительства
Кем выдан паспорт
Когда выдан
Номер домашнего телефона
Номер рабочего телефона
Дети (дата рождения)
Знание иностранных языков (язык, степень знания)
Состав семьи (степень родства, ФИО, год рождения)
Образование (название учебного заведения, тип учебного заведение)

Разряд
Серия и номер диплома, Регистрационный номер диплома
Специальность по диплому
Квалификация по диплому
Дата окончания
Постдипломная подготовка первичная (специальность, форма, дата выдачи удостоверения, дата выдачи сертификата)
Постдипломная подготовка вторичная (специальность, форма, дата выдачи удостоверения, дата выдачи сертификата)
Квалификационная категория (специальность, категория, номер приказа, дата присвоения)
Учёная степень, Специальность, Дата присвоения
Начало медицинского стажа (предыдущая трудовая деятельность) (должность, основная/совмещаемая, номер приказа, дата назначения)
Текущая трудовая деятельность (наименование структурного подразделения, тип должности, место работы, должность, специальность, основная/совмещаемая, номер приказа, объём работы (количество ставок), дата назначения)
Постоянные надбавки и доплаты за интенсивность и дополнительную работу (должность, объём в %)
Правительственные, ведомственные и краевые наград и поощрения (название, дата получения)
Дата начала трудового стажа
ДЛО (имеет ли право на выписку льготных рецептов, дата начала, дата окончания)
Федеральный регистр (дата начала работ, дата окончания работ, причина исключения, население, тип участка, малокомплектный участок, №акта, малокомплектный участок, дата
История невыплат (причина, дата начала периода невыплат, дата окончания периода невыплат)
Воинский учёт (состоит или нет, причина снятия с учёта, дата снятия с учёта, категория запаса, воинское звание, состав, полное кодовое обозначение ВУС (военно-учётная специальность), категория годности к воинской службе, наименование РВК по месту жительства, номер команды, партии)

5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:

На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **3 класса (К3)**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему
АИС «Заработная плата»
установила:
1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес по регистрации, вид документа, удостоверяющего личность, серия и номер этого документа, наименование или код органа, выдавшего документ, дата выдачи документа, индивидуальный номер налогоплательщика (ИНН), серия и номер полиса ОМС, СНИЛС застрахованного, сведения о страховом свидетельстве, номер телефона, стаже работы, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до 1000 записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС
– ФИО, пол, дата и место рождения, адрес места жительства, адрес по регистрации,
– вид документа, удостоверяющего личность, серия и номер этого документа, наименование или код органа, выдавшего документ, дата выдачи документа, адрес по регистрации,
– вид документа, удостоверяющего личность, серия и номер этого документа, наименование или код органа, выдавшего документ, дата выдачи документа,
– индивидуальный номер налогоплательщика (ИНН),
– серия и номер полиса ОМС, СНИЛС застрахованного, сведения о страховом свидетельстве,
– номер телефона, стаж работы;
5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г.№55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **3 класса (К3)**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
–
Рассмотрев исходные данные на информационную систему информационную систему **АИС «Персонифицированный учет для ПФ РФ»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес по регистрации, вид документа, удостоверяющего личность, серия и номер этого документа, наименование или код органа, выдавшего документ, дата выдачи документа, индивидуальный номер налогоплательщика (ИНН), серия и номер полиса ОМС, СНИЛС застрахованного, сведения о страховом свидетельстве, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до 1000 записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС
– Страхователь, Табельный номер, ФИО, Страховой номер, Год отчета
– Задолженность по уплате страховых взносов на начало расчётного периода (на страховую и накопительную часть)
– Начислено страховых взносов за расчётный период (на страховую и накопительную часть)
– Уплачено страховых взносов (на страховую и накопительную часть)
– Задолженность по уплате страховых взносов на конец расчётного периода (на страховую и накопительную часть)
5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. №55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **3 класса (К3)**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему **АИС «Программа по льготникам ПФ РФ»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес по регистрации, вид документа, удостоверяющего личность, серия и номер этого документа, наименование или код органа, выдавшего документ, дата выдачи документа, индивидуальный номер налогоплательщика (ИНН), серия и номер полиса ОМС, СНИЛС застрахованного, сведения о страховом свидетельстве, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до 1000 записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС
– Подразделение, Наименование, Количество, ЛПУ, Страховой номер
– ФИО
– Должность
– Доход
– Перечисленные взносы в ПФР
5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **3 класса (К3)**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему **ИС «Арбитражные исследования»**

установила:
1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес по регистрации, сведения о лабораторных исследованиях на ВИЧ, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до **100000** записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС
– № пациента, ФИО, Пол, Год рождения
– Район, Населённый пункт, Улица, Дом, квартира
– № забора крови, Дата взятия, Дата поступления
– Качество образца, ЛПУ забора крови
– Дата результатов исследования (ИБ)
– Тест-система (ИБ) , Результат (ИБ) , Расшифровка белков
– Дата результатов исследования (ИФА) , Тест-система (ИФА) ,Результат (ИФА)
– Оптическая плотность
– Группа D-учёта, Группа контингента
– Комментарий к результату
– Расшифровка результата
5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. №55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **ИСПД 1 класса**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему «**Электронный журнал по иммунологическим исследованиям»**

установила:
1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес места жительства, сведения о иммунологических исследованиях, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – до 10000записей.
3. Заданные характеристики безопасности персональных данных – типовые.
4. Структура ИС
– Дата, номер
– ФИО
– Дата забора материала, Дата поступления
– Дата рождения, Возраст на дату, Пол, Адрес
– Диагноз
– ЛПУ (забор материала)
– Лаборатория, проводившая исследование
– ФИО врача (направл.), Контактный телефон
– Относительное количество в процентах (лимфоциты, СД3, СД4, СД8)
– Абсолютное количество (лейкоциты, лимфоциты, СД3, СД4, СД8)
– Факт сохранения плазмы
– Дата выполнения анализа, Врач-лаборант
– Количество биологического материала
5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – без подключения>.
6. Режим обработки персональных данных – однопользовательский.
7. Права доступа к персональным данным (полномочия) пользователей – < равные>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **ИСПД 1 класса**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему «**Электронный журнал по ПЦР-исследованиям»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес места жительства, сведения о лабораторных ПЦР исследованиях, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до* 10000 *записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС

– № документа, Дата поступления, Дата забора материала
– ФИО клиента, Дата рождения, Возраст на дату, Пол
– Д-учёт, Адрес, Диагноз
– ЛПУ (забор материала) , Лаборатория (1 иссл.)
– ФИО врача (направл.) , Врач-лаборант
– Срок беременности, День цикла, Медик
– Опред. показатель
– Заключение, Результат, Ед. изм. , Реф. пределы
– Дата выполнения
– Вид биологического материала, Качество биологического материала

5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **ИСПД 1 класса**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему **«Программа по диспансеризации детей»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес места жительства, адрес по регистрации, результаты лабораторных исследований, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до* 1000 записей.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС

– № по порядку, ФИО, Пол, Дата рождения
– Дата взятия на учёт, Район/город, Адрес, Группа, Подгруппа
– Путь заражения, Окончательный диагноз, Дата установления окончательного диагноза
– Дата снятия с учёта, Предполагаемая дата снятия с учёта
– Химиопрофилактик, Способ родоразрешения, Вид опеки
– ЛПУ, осуществляющее наблюдение
– Сведения о родителях (мать, отец) (ФИО, дата ИБ, № ИБ, статус, код) , Код
– Результат обследования ИФА, ИБ, ПЦР, ПЦР (РНК) (наименование, дата, результат)
– Результаты дополнительных методов обследования, Стадия заболевания
– Вес, Рост, Оценка по Абгар, Окружность головы, Окружность груди, Диагноз
– Вскармливание, Данные объектного осмотра

5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **ИСПД 1 класса**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему **«Программа по Д-учету беременных женщин»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес места жительства, другие сведения, предусмотренные федеральными законами и трудовыми отношениями;
2. Объем обрабатываемых персональных данных – *до* 1000*записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС

– Эпид. номер, ФИО, Дата рождения, Район, город, Адрес, Путь инфицирования, Статус
– Химиопрофилактика
– Состояние на учёте, Дата обращение в ЖК, Дата взятия на учёт
– Место состояния на учёте
– Срок беременности на момент взятия на учёт
– Срок беременности на сегодняшний день
– Предполагаемая дата родов
– Дата снятия с учёта
– Аборт (роды)

5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *однопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **ИСПД 1 класса**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему **«Программа по Д-учету ВИЧ-инфицированных»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес места жительства, адрес по регистрации, другие сведения;
2. Объем обрабатываемых персональных данных – *до* 100000 *записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС

– Эпид. номер, диспансерный номер, Пол, Дата рождения, Год рождения, Гражданство
– Адрес места жительства выявления (край/область, район/город, МГЗ, домашний адрес)
– Адрес места жительства фактический(край/область, район/город, МГЗ, домашний адрес)
– Дата ИБ
– Код обследования (группа обследования)
– Код контингента (причина заражения)
– Путь передачи
– Дата снятия
– Информация о выбытии (дата, территория, адрес)
– Информация о смерти (дата, причина)
– Дата прибытия (с другой территории с диагнозом “ВИЧ-инфекция”)
– Территория
– Район, город (ф.)
– Дата первичного выявления, Эпид. № первичного выявления
– Дата раскодировки анонима
– Социальное положение, Статус
– Место работы или учёбы, службы, Должность
– Группа инвалидности по ВИЧ-инфекции
– Дата взятия на учёт
– Информация о иммуноблоте (дата, номер и результат)
– Информация о рецепиентах (ФИО, год рождения, адрес, гемотрансфузия, ВИЧ, №, Rrez)
– Сроки нахождения в учреждениях УФСИН (начало, конец, название УФСИН, лечение)
– ЛПУ по месту жительства
– Дата передачи в ЛПУ по месту жительства
– Дата взятия на Д-учёт в ЛПУ
– Дата запроса в городское/районное УФ МС о наличии регистрации (не вставших на учёт)

- Дата предоставления ЛПУ в краевой Центр СПИД списков незарегистрированных в городе (районе)
- Дата запроса АКЦПБ со СПИДом в краевое УФ МС о наличии регистрации в крае
- Дата ответа из краевого УФ МС
- Дата запроса ЛПУ в РОВД по розыску не проживающих по указанному адресу
- Дата ответа из РОВД
- Дата предоставления в АКЦПБ со СПИДом списков ВИЧ(+), на которых получено 2 ответа из РОВД
- Дата снятия с учёта, Стадия ВИЧ 2005, Стадия ВИЧ 2001, Лечащий врач
- Дата перехода из группы в группу, Дата отказа от Д-наблюдения
- Соп. заболевания (код, дата установления наблюдения, дата снятия наблюдения, расшифровка)
- Оказание помощи (начало, окончание, тип помощи, где оказывалась, ЛПУ (место оказания))
- Дата отказа от ВААРТ
- Схемы терапии (лечение, начало приёма, окончание приёма, схема терапии, проект, прекращение приёма)
- Выданные препараты (дата выдачи, место выдачи, количество, название, серия, срок, фонд)
- СД-4 (№, дата, количество, группа)
- РНК ВИЧ (№, дата, количество, группа)
- Флюорография органов грудной клетки (№, дата, результат)
- Проба Манту с 2ТЕ (№, дата, результат)
- Гепатиты (дата, HbsAg, HbeAg, aHCV, качественно, генотип, количественно, ДНК ВГВ)
- Общий анализ крови (дата, гемоглобин, эритроциты, лейкоциты, э, б, п, с, м, л)
- Общий анализ мочи (РОЭ, лимф, тромбоциты, удельный вес, белок, сахар, УЗИ)
- Биохимический анализ (дата, АЛТ, АЛТ (показ), АСТ, щел. фосфотаз, бил. общ, бил. прям, аминолаза, тимол. пр, глюкоза, холестерин, альбумин, креатинин, мочевина, общ. белок)

5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *многопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *разные*>.

РЕШИЛА:

На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **ИСПД 1 класса**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

АКТ
классификации информационной системы персональных данных
Краевого государственного бюджетного учреждения здравоохранения
Алтайский краевой Центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями

Комиссия в составе:
Председатель:
– ***Е.Б.Поподьина***
Члены комиссии:
– ***А.М.Домашец, С.А.Драчков***
Рассмотрев исходные данные на информационную систему информационную систему **«Программа по Д-учету контактных, серопозитивных»**

установила:

1. ИС содержит персональные данные – фамилия, имя, отчество, пол, дата и место рождения, адрес места жительства, другие сведения;
2. Объем обрабатываемых персональных данных – *до* 100000 *записей*.
3. Заданные характеристики безопасности персональных данных – *типовые*.
4. Структура ИС

– Номер, ФИО, Пол, Год рождения
– Код
– Группа
– Район/город, Населённый пункт, Адрес
– Место работы
– Должность
– Передающая лаборатория
– Состояние
– Постановка
– Снятие
– Поликлиника

5. Наличие подключения к сетям и системам общего пользования и сетям международного информационного обмена (Интернет) – *без подключения*>.
6. Режим обработки персональных данных – *многопользовательский*.
7. Права доступа к персональным данным (полномочия) пользователей – < *равные*>.

РЕШИЛА:
На основании приказа ФСТЭК от 13 февраля 2008г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" присвоить информационной системе персональных данных **ИСПД 1 класса**;

Председатель комиссии ***Е.Б.Поподьина***

Члены комиссии: ***А.М.Домашец***

С.А.Драчков

Приложение 3

Список сотрудников, за которыми установлена персональная ответственность за обеспечение сохранности, конфиденциальности и безопасности в ходе обработки персональных данных

Начальник отдела информации – Поподьина Е.Б.
Инженер-программист – Драчков С.А.
Инженер-программист – Мамонова Т.Ю.
Инженер-электроник – Павлушов Е.И..

Приложение 4

Должностные обязанности администратора информационной безопасности

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности ГУЗ Алтайского краевого центра по профилактике и борьбе со СПИДом и инфекционными заболеваниями.
1.2. Администратор информационной безопасности является штатным сотрудником отдела автоматизированной обработки информации (далее АОИ), назначается приказом главного врача ГУЗ АКЦПБ со СПИДом по представлению заведующего отдела АОИ.
1.3. Администратор информационной безопасности подчиняется непосредственно заведующему отдела АОИ.
1.4. На время отсутствия администратора безопасности ГУЗ АКЦПБ со СПИДом его обязанности выполняет лицо, назначенное в установленном порядке. Данное лицо приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.
1.5. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора информационной безопасности.
1.6. Администратор информационной безопасности обладает правами доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей и средствам их защиты.

2. Обязанности администратора информационной безопасности

2.1. Знать перечень установленных в подразделениях ГУЗ АКЦПБ со СПИДом рабочих станций и перечень задач, решаемых с их использованием.
2.2. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных рабочих станций (РС) и автоматизированных систем (АС).
2.3. Осуществлять оперативный контроль за работой пользователей защищенных РС, анализировать содержимое системных журналов всех РС и адекватно реагировать на возникающие нештатные ситуации.
2.4. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на РС АС специальных технических средств защиты от несанкционированного доступа (НСД).
2.5. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных РС и серверов, устанавливать и осуществлять настройку средств защиты РС.
2.6. Периодически проверять состояние используемых средств защиты информации (СЗИ) НСД, осуществлять проверку правильности их настройки (выборочное тестирование).
2.7. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных РС.
2.8. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам ПЭВМ.

2.9. Докладывать руководству службы обеспечения информационной безопасности об имевших место попытках несанкционированного доступа к информации и техническим средствам ПЭВМ.
2.10. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от НСД, установленных на РС АС.
2.11. Проводить занятия с сотрудниками и администраторами безопасности подразделений по правилам работы на ПЭВМ, оснащенных СЗИ НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации.
2.12. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.
2.13. Осуществлять антивирусный контроль.
2.14. Участвовать в работе комиссий по пересмотру Планов защиты.

3. Права администратора информационной безопасности

3.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АС.
3.2. Непосредственно обращаться к руководителям подразделений с требованием прекращения работы в АС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.
3.3. Вносить свои предложения по совершенствованию мер защиты в АС.

4. Ответственность администратора информационной безопасности

4.1. На администратора информационной безопасности возлагается персональная ответственность за программно - технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним приказом главного врача ГУЗ АКЦПБ со СПИДом за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.
4.2. Администратор информационной безопасности несет ответственность по действующему законодательству за разглашение сведений, составляющих (государственную, банковскую, коммерческую) тайну, и сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение 5

Список сотрудников, на которых возложены обязанности администратора информационной безопасности:

Программист – Драчков С.А.

Приложение 6

Инструкция по проведению антивирусного контроля

Инструкция

по проведению антивирусного контроля на объекте вычислительной техники (ОВТ) - автоматизированное рабочее место

1. Настоящая Инструкция предназначена для Администратора информационной безопасности и пользователей, обрабатывающих информацию на ОВТ.
2. В целях обеспечения антивирусной защиты на ОВТ производится антивирусный контроль.
3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Администратора информационной безопасности информации.
4. К применению на ОВТ допускаются лицензионные антивирусные средства.
5. На ОВТ запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ.
6. Пользователи ОВТ при работе с носителями информации обязаны перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.
7. Ярлык для запуска антивирусной программы должен быть вынесен на "Рабочий стол" операционной системы.
8. Администратор информационной безопасности один раз в неделю осуществляет установку пакетов обновлений вирусных баз, осуществляет контроль их подключения к антивирусному пакету и проверку жесткого диска и съемных носителей на наличие вирусов.
9. При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Администратора информационной безопасности и прекратить какие-либо действия на ОВТ.
10. Администратор информационной безопасности проводит расследование факта заражения ОВТ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путем выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.
11. В случае обнаружения не поддающегося лечению вируса, Администратор информационной безопасности обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность ОВТ. В случае отказа ОВТ – произвести восстановление соответствующего программного обеспечения.

Приложение 7

Инструкция по организации парольной защиты в АС

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в учреждении ГУЗ АКЦПБ со СПИДом, а также контроль за действиями пользователей при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на всех рабочих станциях и автоматизированных системах ГУЗ АКЦПБ со СПИДом и контроль за действиями пользователей при работе с паролями возлагается на сотрудников, несущих персональную ответственность за обеспечение сохранности, конфиденциальности и безопасности в ходе обработки персональных данных (*Приложение 3).*

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 6 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочей станции, автоматизированной системы и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается сотрудников, несущих персональную ответственность за обеспечение сохранности, конфиденциальности и безопасности в ходе обработки персональных данных (*Приложение 3)*. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

4. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п., а также в случае технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие пароли должны быть заменены.

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри ГУЗ АКЦПБ со СПИДом и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального органа ГУЗ АКЦПБ со СПИДом и другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

8. В случае компрометации личного пароля пользователя, должны быть немедленно предприняты меры в соответствии с п.6 или п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в запечатанном конверте.

10. Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на сотрудников– администраторов средств парольной защиты.

Приложение 8

Должностные обязанности программиста

ГУЗ «Алтайский краевой центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями»

УТВЕРЖДАЮ:
Главный врач
_____Л. В. Султанов

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

«___» _____2015 г.

инженера-программиста
«____» _____2015 г. № _____

Общие положения.

На должность инженера-программиста назначается:

Программист – высшее профессиональное образование без предъявления требований к стажу работы;

Программист П категории – высшее профессиональное образование и стаж работы в должности программиста не менее 3 лет;

Программист 1 категории – высшее профессиональное образование и стаж работы в должности программиста П категории не менее 3 лет;

Ведущий программист – высшее профессиональное образование и стаж работы в должности программиста 1 категории не менее 3 лет.

1. Основной задачей инженера-программиста является разработка программ, реализующих решение задач для осуществления целевой деятельности Центра.
2. Инженер-программист в своей работе руководствуется:

- руководящими нормативными материалами,
- правилами технической эксплуатации вычислительной техники,
- технологией электронной обработки информации,
- правилами внутреннего трудового распорядка, техники безопасности и противопожарной защиты,
- указаниями заведующего отделом,
- настоящей должностной инструкцией.

3. Инженер-программист подчиняется главному врачу Центра, руководителю структурного подразделения, назначается, перемещается и освобождается от должности согласно действующему законодательству и коллективному договору.

ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Инженер-программист обязан:

1. Разрабатывает на основе анализа математических моделей и алгоритмов решения экономических и других задач программы, обеспечивающие возможность выполнения алгоритма и соответственно поставленной задачи средствами вычислительной техники, проводит их тестирование и отладку.
2. Разрабатывает технологию решения задачи по всем этапам обработки информации.
3. Определяет информацию, подлежащую обработке средствами вычислительной техники, ее объемы, структуру, макеты и схемы ввода, обработки, хранения и вывода, методы ее контроля.

4. Осуществляет выбор языка программирования для описания алгоритмов и структур данных.
5. Выполняет работу по подготовке программ к отладке и проводит их отладку.
6. Определяет объем и содержание данных контрольных примеров, обеспечивающих наиболее полную проверку соответствия программ их функциональному назначению.
7. Осуществляет запуск отлаженных программ и ввод исходных данных, определяемых условиями поставленных задач.
8. Проводит корректировку разработанной программы на основе анализа выходных данных.
9. Определяет возможность использования готовых программных продуктов.
10. Разрабатывает инструкции по работе с программами, оформляет необходимую техническую документацию.
11. Осуществляет сопровождение внедренных программ и программных средств.
12. Разрабатывает и внедряет системы автоматической проверки правильности программ.
13. Выполняет работу по унификации и типизации вычислительных процессов.
14. Принимает участие в создании каталогов и картотек стандартных программ, в разработке форм документов в электронном виде, подлежащих компьютерной обработке, в проектировании программ, позволяющих расширить область применения вычислительной техники.
15. Обеспечивает правильную техническую эксплуатацию, бесперебойную работу компьютеров и отдельных устройств.
16. Участвует в разработке перспективных и годовых планов и графиков работы, технического обслуживания и ремонта оборудования, мероприятий по улучшению его эксплуатации, предупреждению простоев в работе, повышению качества работы, эффективному использованию вычислительной техники.
17. Осуществляет подготовку компьютеров и отдельных устройств к работе, их технический осмотр, проводит проверку наличия неисправностей, устраняет неисправности и предотвращает появление неисправностей в будущем.
18. Принимает меры по своевременному и качественному выполнению ремонта компьютеров и отдельных устройств своими силами или силами третьих лиц.
19. Принимает участие в проведении инвентаризаций.
20. Должен беречь имущество предприятия, не разглашать информацию и сведения, являющиеся коммерческой тайной предприятия.
21. Не дает интервью, не проводит встречи и переговоры, касающиеся деятельности предприятия, без разрешения руководства предприятия.
22. Соблюдает трудовую и производственную дисциплину, правила и нормы охраны труда, требования производственной санитарии и гигиены, требования противопожарной безопасности, гражданской обороны.
23. Исполняет распоряжения и приказы Главного врача предприятия и руководителя отдела.
24. Информирует руководство об имеющихся недостатках в работе предприятия, принимаемых мерах по их ликвидации.
25. Способствует созданию благоприятного делового и морального климата предприятия.

ПРАВА

Требовать от заведующего отделом и руководства центра СПИД:

- создания условий труда в соответствии с требованиями техники безопасности и противопожарной защиты,
- своевременной консультации по проводимым разработкам программ, а также информации, необходимой для выполнения поставленных задач.

ОТВЕТСТВЕННОСТЬ

Инженер-программист несет ответственность за:

Некачественную и своевременную разработки программ в соответствии с заданием на программирование.

За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных действующим трудовым законодательством РФ.

За правонарушение, совершенное в процессе осуществления своей деятельности (в том числе за разглашение врачебной тайны), в пределах определенных действующим административным, уголовным и гражданским законодательством РФ.

За сохранность вверенных материальных ценностей и оборудования, необходимых, для осуществления своей деятельности.

Соблюдение правил внутреннего трудового распорядка, правил техники безопасности и противопожарной защиты.

Руководитель структурного_____ _____
подразделения подпись Ф.И.О.
« ____» _____ 2015г.

СОГЛАСОВАНО:
Юрисконсульт
_____ _____ «___»_____2015г.
подпись Ф.И.О.

С инструкцией ознакомлен (а):

_____ _____ «____»_____2015 г.

Приложение 9

Инструкция о порядке еженедельного технического обслуживания персонального компьютера для пользователя

1. Общие положения

Техническое обслуживание это комплекс работ направленных на поддержание машин и оборудования в работоспособном состоянии в течении периода эксплуатации. Техническое обслуживание (ТО) персонального компьютера (ПК) подразделяется на еженедельное (ЕТО), полугодовое (ПТО), годовое (ГТО). Еженедельное техническое обслуживание (ЕТО) проводиться пользователем или лицом ответственным за ПК. Полугодовое, годовое ТО проводиться инженером-электроником.

Инструкция по еженедельному техническому обслуживанию должна находиться на каждом рабочем месте.

2. Перечень работ ЕТО

2.1. Осмотр состояния кабелей, розеток, разъемов.

2.2. Удаление загрязнений с внешних поверхностей блоков: клавиатуры, мышки, монитора, принтера (очистка внутренних узлов и деталей производиться в момент заправки в отделе АОИ), сканера, модема.

2.3. Диагностика ПК:

2.3.1. Проверка на наличие вирусов,

2.3.2. Очистка диска от временных и не используемых файлов,

2.3.3. Дефрагментация диска,

2.3.4. Проверка работоспособности клавиш клавиатуры и манипулятора,

2.3.5. Пробная печать на принтере.

2.3.6.Проверка работоспособности сетевого подключения осуществляется набором команды

« ping <IP-адрес или имя компьютера>» используя команду "Выполнить" в меню "Пуск":

« ping 192.168.0.1» для компьютеров подключенных к ЛВС подразделения через сетевой адаптер.

При исправном соединении выдается время прохождения пакета (<1мс).

3. Действия персонала при обнаружении неисправностей

При выполнении диагностики ПК выявляются неисправности устройств ПК и программного обеспечения. Для устранения выявленных неисправностей необходимо обращаться в отдел АОИ (ремонтом вычислительной техники занимается только отдел АОИ.)

4. Используемые материалы при выполнении работ

Для удаления загрязнений в виде пыли с пластмассовых и металлических поверхностей используется ткань или специальные салфетки.

С поверхности монитора пятна и пыль удаляются специальными салфетками или специальными жидкостями. Въевшиеся отложения с пластмассовых поверхностей удаляются специальными салфетками. Запрещается использовать для очистки мониторов с антибликовыми покрытиями любые растворы.

5. Сроки и время проведения ТО

Еженедельное техническое обслуживание ПК проводиться пользователем не реже 1 раза в неделю в один и тот же день недели. Сроки и время предоставления ПК для проведения полугодового и годового обслуживания согласуется с отделом АОИ.

6. Техника безопасности при проведении работ

6.1. Перед удалением загрязнений поверхностей компьютера устройства ПК необходимо выключить.
6.2. При обнаружении повреждений электрических розеток, кабелей в т.ч. заземления необходимо срочно вызвать электрика.
6.3. Запрещается при проведении ТО:
использовать для очистки жесткие предметы (авторучки, карандаши, ножи, линейки и др.),
подключать и отключать устройства ПК при включенном электропитании,
открывать блоки (работы по очистке внутренних узлов осуществляются специалистами отдела АОИ при проведении полугодового и годового ТО)

7. Рекомендации
Если пользователь не уверен в своих знаниях по работе с компьютером, с программами следует обратиться для получения консультации в отдел АОИ.

8. Ответственность
Пользователь несет персональную ответственность за нарушение правил эксплуатации ПК и в т.ч. нарушение проведения сроков и перечня работ по ЕТО и предоставлению на полугодовое и годовое ТО.

Приложение 10

Перечень защищаемых информационных ресурсов

1. АИС «Кадры здравоохранения»;
2. АИС «Заработная плата»;
3. АИС «Персонифицированный учет для ПФ РФ»;
4. АИС «Программа по льготникам ПФ РФ».

ИСПДн пациентов (лаборатория):

5. ИС «Арбитражные исследования»;
6. Электронный журнал по иммунологическим исследованиям;
7. Электронный журнал по ПЦР-исследованиям.

ИСПДн пациентов (лечебный отдел):

8. Программа по Д-учету ВИЧ-инфицированных;
9. Программа по диспансеризации детей;
10. Программа по Д-учету беременных женщин;
11. Программа по Д-учету контактных, серопозитивных.

Приложение 11

План размещения АРМ, на которых осуществляется обработка персональных данных

Схема расположения компьютеров, подлежащих защите,
в кабинетах лечебного отдела

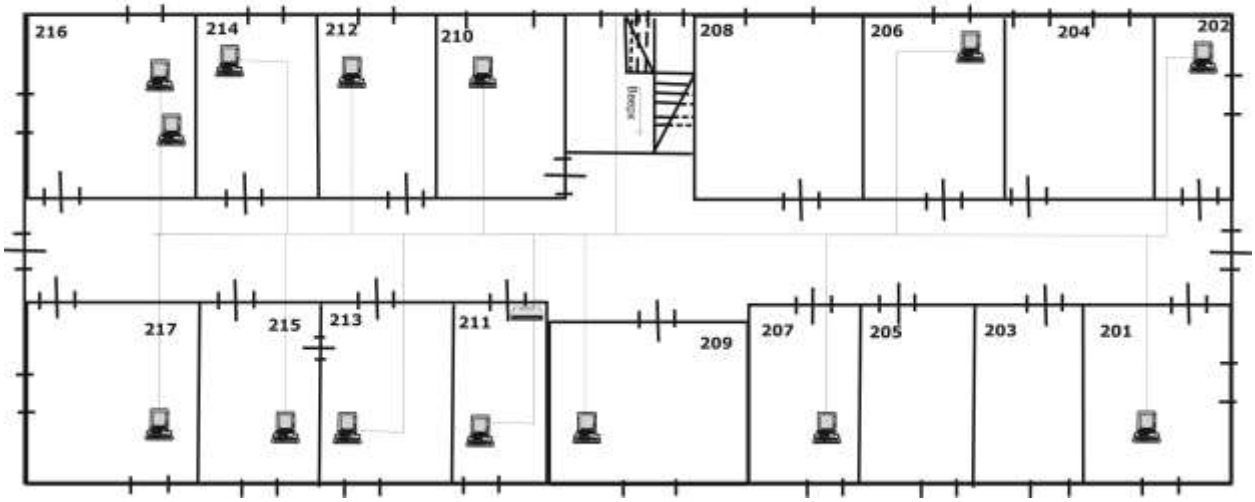


Схема расположения компьютеров в кабинетах лаборатории

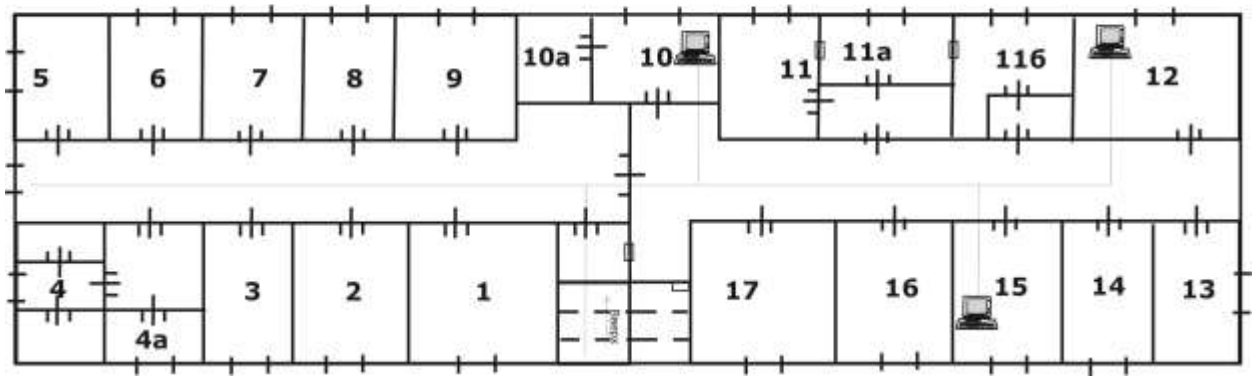
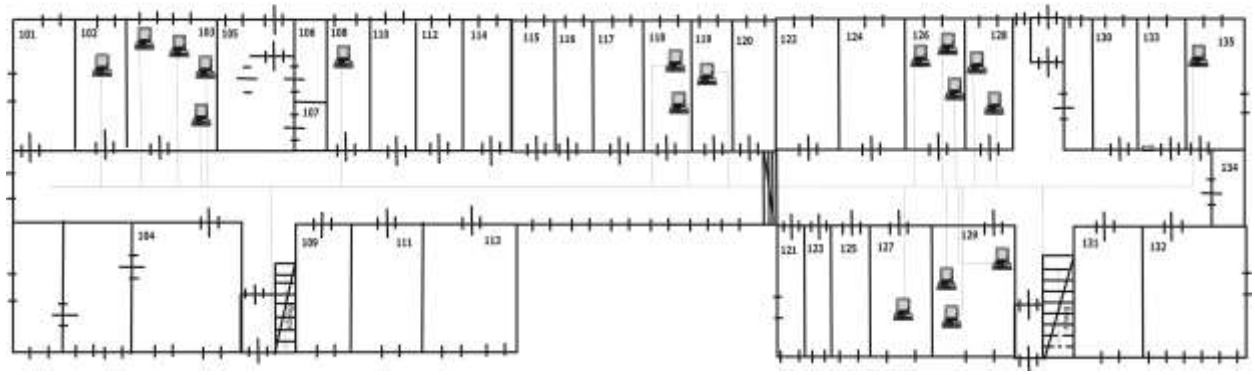


Схема расположения компьютеров, подлежащих защите,
в кабинетах 1-го этажа



Приложение 12

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации

I. Общие положения

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Алтайского края, а также правовыми актами ГУЗ «Алтайский краевой центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями», должны применяться с учетом требований настоящего Положения.

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

5. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Алтайского края, а также правовыми актами ГУЗ «Алтайский краевой центр по профилактике и борьбе со СПИДом и инфекционными заболеваниями».

7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес организации-оператора, фамилию, имя, отчество лица, осуществляющего обработку персональных данных без использования средств автоматизации, фамилию, имя, отчество

и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

9. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

12. Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, либо путем изготовления нового материального носителя с уточненными персональными данными.

III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним

доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются главным врачом учреждения.

Приложение 13

Журнал учета мероприятий
по контролю за системой обеспечения безопасности персональных данных

Дата и время проведения мероприятий по контролю	Дата и № распоряжения	Наименование органа государственного контроля (надзора)	Цели, задачи и предмет мероприятия по контролю, правовые основания	Сведения о выявленных нарушениях, о составленных протоколах, об административных правонарушениях и выданных предписаниях	ФИО, должность лица (лиц), № служебного удостоверения	Подпись лица, проводившего проверку

Приложение 14

Журнал учёта организационно-распорядительных документов,
касающихся обработки персональных данных

№ п/п	Регистрационный номер и дата документа	Наименование документа и краткое содержание (тема документа)	ФИО ответственного за исполнение	Пометка об исполнении

Приложение 15

Инструкция пользователя по защите информации при работе с базами данных

В настоящей Инструкции использованы следующие термины и определения:

1. База данных (далее – БД) – централизованное хранилище информации, оптимизированное для многопользовательского доступа и работающее под управлением системы управления базами данных (далее – СУБД).

2. Информационная система с использованием БД (далее – ИСБД) – система или приложение, использующее непосредственный доступ к БД.

3. Идентификатор – буквенно-числовая последовательность, позволяющая однозначно определять работу пользователя в БД.

4. Пароль – секретная последовательность символов, известная только пользователю, позволяющая подтвердить соответствие реальной сущности пользователя, предъявляемая им идентификатору.

5. Пользователи – должностные лица АКЦПБ со СПИДом, а также все другие лица , работающие с БД АКЦПБ со СПИДом.

6. Администратор БД и администратор информационной безопасности – должностные лица АКЦПБ со СПИДом, уполномоченные для выполнения административных функций и обеспечивающие функционирование БД и ее безопасность соответственно.

7. ЛВС – локальная вычислительная сеть.

8. Политика информационной безопасности – комплекс организационно-технических мероприятий, правил и условий использования информационных систем АКЦПБ со СПИДом, определяющих нормальное функционирование систем и обеспечение безопасности информации, обрабатываемой в АКЦПБ со СПИДом, оформленных в виде нормативных документов.

Общие положения по организации доступа к базам данных АКЦПБ со СПИДом

9. Инструкция пользователя по защите информации при работе с базами данных АКЦПБ со СПИДом (далее – Инструкция) определяет комплекс организационно-технических мероприятий по обеспечению безопасности информации, хранящейся в БД и обрабатываемой с помощью средств вычислительной техники в ЛВС.

10. Инструкция предназначена для обеспечения эффективной организации и управления доступом пользователей к информации, хранящейся в БД, и содержит требования по обеспечению информационной безопасности в АКЦПБ со СПИДом в части выполнения операций по организации и управлению доступом к БД.

11. Инструкция является частью политики информационной безопасности АКЦПБ со СПИДом.

12. Обеспечение информационной безопасности работы АКЦПБ со СПИДом в части организации и управления доступом к БД основывается на требованиях следующих руководящих документов:

– Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных»

– Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

– ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ от 17 ноября 2007 г. N 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

– УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ «Об утверждении перечня сведений конфиденциального характера» (в ред. Указа Президента РФ от 23.09.2005 N 1111)

– Приказ главного Управления АЛТАЙСКОГО КРАЯ ПО ЗДРАВООХРАНЕНИЮ И ФАРМАЦЕВТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ «Об организации защиты персональных данных регионального сегмента Федерального регистра лиц в лечебно-профилактических учреждениях и аптечных организациях», №498 от 27.12.2007

– Приказ главного Управления АЛТАЙСКОГО КРАЯ ПО ЗДРАВООХРАНЕНИЮ И ФАРМАЦЕВТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ «О проведении работ по защите персонифицированной информации в учреждениях здравоохранения края» №425 от 24.07.2008г.

13. Требования Инструкции обязательны для выполнения всеми пользователями. Ответственность за выполнение требований Инструкции несут пользователь БД и начальник подразделения, в котором работает данный пользователь. Перед началом работы пользователь обязан ознакомиться с данной Инструкцией.

14. Все положения Инструкции, упоминающие подключение к БД, распространяются также и на подключение к ИСБД, если иное не оговорено явно в тексте Инструкции.

15. Решение задач, связанных с организацией и управлением доступом должностных лиц АКЦПБ со СПИДом к БД, осуществляется администратором баз данных совместно с администратором информационной безопасности. При возникновении ситуаций, не описываемых положениями настоящей Инструкции, решение принимает администратор БД совместно с администратором информационной безопасности, руководствуясь Инструкцией администратора информационной безопасности.

16. Ответственность за сохранность и правильное использование информации, полученной из БД, несут пользователь, имеющий доступ к БД, и начальник структурного подразделения, в составе которого работает пользователь. Ответственность наступает с момента поступления информации на рабочую станцию пользователя, фиксируемого в протоколе аудита БД.

17. Для обеспечения доступа пользователей к БД на их рабочих станциях должно быть установлено специальное программное обеспечение, обеспечивающее доступ и выполнение операций с информацией в БД. Установку и конфигурирование данного программного обеспечения на рабочих станциях пользователей выполняет администратор БД.

18. Пользователям запрещается самостоятельно устанавливать другое программное обеспечение (или менять параметры конфигурации ранее установленных программных средств) для доступа и манипулирования данными в БД.

19. Доступ пользователей к БД предоставляется только с использованием учетной записи, которая выдается администратором БД, по указанию начальника структурного подразделения. Запрещается предоставлять пользователям доступ к информации, хранящейся в БД, способами, отличными от вышеуказанного.

20. Доступ к БД предоставляется исключительно пользователям, прошедшим регистрацию в ЛВС АКЦПБ со СПИДом.

Идентификация и авторизация пользователей

21. Для каждого из пользователей, которым необходим доступ к БД, создается учетная запись о пользователе БД, состоящая из имени (идентификатора) пользователя и пароля.

22. Срок действия активной учетной записи пользователя БД 1 год. Срок действия учетной записи пользователя должен периодически продлеваться согласно нижеследующей процедуре, иначе учетная запись блокируется до принятия положительного решения о продлении полномочий пользователя.

23. Значение пароля устанавливает администратор БД. Периодичность, порядок и технология изменения пароля доводится администратором безопасности БД до пользователей.

24. Не допускается использование различными пользователями одной и той же учетной записи. Это правило действует и в тех случаях, когда пользователи имеют одинаковые полномочия по доступу к БД. Для ИСБД данное положение может не применяться, если в технологической схеме есть прямое указание на возможность коллективного использования одной учетной записи.

Порядок организации доступа пользователей к базам данных

25. Порядок организации доступа к БД:

Заведующий отделом автоматизированной обработки информации АКЦПБ со СПИДом или его заместитель принимает решение о разрешении доступа пользователя к БД по ходатайству заведующего структурного подразделения АКЦПБ со СПИДом, в составе которого работает данный пользователь.

Заведующий структурным подразделением составляет заявку на регистрацию/изменение/удаление пользователя баз данных, выполняя действия в следующем порядке:

– заносит заявку в «журнал регистрации/изменении/удалении заявок доступа к БД»;

– согласует ее с заведующим ОАОИ или его заместителем;

– передает ее администратору БД.

Администратор БД лично сообщает пользователю его идентификатор и пароль для доступа к БД под роспись в журнале регистрации/изменении/удалении паролей.

Решение о необходимости изменения полномочий доступа пользователя к БД принимает заведующий ОАОИ по ходатайству заведующего структурного подразделения, в составе которого работает данный пользователь, на основании заявки на изменение полномочий пользователя БД. За 1 месяц до окончания срока действия полномочий пользователя заведующий структурным подразделением направляет заявку на продление полномочий пользователя в ОАОИ.

Решение об удалении учетной записи пользователя БД принимает заведующий ОАОИ или его заместитель по представлению администратора БД или администратора информационной безопасности на основании заявки заведующего структурным подразделением, в составе которого работает данный пользователь.

26. Пользователю запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа к БД другим лицам, в том числе и своим руководителям. Запрещается хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле.

27. Пользователю запрещается использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями и технологическими схемами.

Обязанности пользователей баз данных

28. Пользователь, имеющий возможность ввода или изменения данных в БД, обязан обеспечить правильность вводимых данных.

29. Пользователь обязан закрывать соединение с базой данных на время своего отсутствия у рабочей станции.

30. Пользователь или заведующий структурным подразделением обязаны своевременно сообщать администратору баз данных об изменениях статуса пользователя (увольнение, перевод на другую должность и т.п.).

31. В случае выявления инцидентов с доступом к БД (фактов несанкционированного доступа к БД, блокировки доступа, утери или компрометации пароля и т.д.) пользователь обязан незамедлительно сообщить об этом администратору БД или администратору информационной безопасности.

32. Возможность подключения к БД не дает права пользователям подключаться к БД, если им не предоставлены права доступа к этим БД. Такие подключения рассматриваются как попытки несанкционированного доступа.

Ответственность пользователей баз данных

33. При нарушениях правил, связанных с информационной безопасностью, пользователь несет ответственность, установленную действующим законодательством Российской Федерации.

34. Пользователь несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования учетной записи.

35. Заведующие структурных подразделений несут персональную ответственность за неправильное использование личным составом учетных записей пользователей, имеющих доступ к БД АКЦПБ со СПИДом, а также за ознакомление (под роспись) с Инструкцией новых пользователей БД в своем структурном подразделении.

36. При выявлении инцидентов с доступом к БД доступ пользователей к БД может быть приостановлен до окончания расследования инцидента, о чем пользователь либо его руководитель уведомляются в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к БД, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к административной ответственности.

Приложение 16

Журнал регистрации запросов субъектов персональных данных на предоставление доступа к персональным данным

№ п/п	Подразделение	№ каб	ФИО руководителя подразделения	ФИО сотрудника, работающего с персональными данными	Специальность сотрудника, работающего с персональными данными	Роспись руководителя подразделения

Приложение 17

Перечень помещений, на которых производится обработка персональных данных

1. Лаборатория – каб. №10, 12, 15
2. Отдел клинической эпидемиологии– каб. №108,118, 128
3. ОАОИ - каб. 126, 129
4. Бухгалтерия - каб. 102, 103
5. Отдел кадров –каб.119
6. Лечебный отдел –каб.№201, 202, 206, 207, 209, 210, 211, 212, 213, 214, 215, 216, 217, 135, 127

В вышеперечисленных помещениях:

- Исключить неконтролируемое пребывание лиц, не имеющих право доступа к информационным ресурсам;
- В случае обнаружения факта несанкционированного проникновения в ВП посторонних лиц производится расследование, с обязательным составлением акта;
- Уборка помещений должна осуществляться в присутствии одного из работников данного помещения.

Приложение 18

Перечень помещений, вход в которые должен быть ограничен от лиц, не имеющих отношения к работе с персональными данными

1. Лаборатория – каб. №11, 12, 15
2. Эпид. отдел – каб. № 118, 128
3. ОАОИ - каб. 129
4. Бухгалтерия - каб. 103, 102
5. Отдел кадров –каб.119

Приложение 19

Форма журнала учета мероприятий по контролю за исполнением правил обработки персональных данных

№ п/п	Дата мероприятия	ФИО проверяющего	ФИО ответственного за исполнение	Замечания и предложения
1.	2.	3.	4.	5.

Приложение 20

Ответственные лица, за которыми закрепляются компьютеры

№ Кабинета	Подразделение	Лица, допущенные к работе на компьютере
10	Лаборатория	Торовкова Т.В.
12	Лаборатория	Алёхина Л.Н.
15	Лаборатория	Дюканова О.И.
109	Отдел клинической эпидемиологии	Николенко А.А.
118	Отдел клинической эпидемиологии	Минакова М.В., Попова В.В., Щербинина Ю.О.
128	Отдел клинической эпидемиологии	Коломоец Ю.П., Глумова А.Е.
129	ОАОИ	Поподьина Е.Б., Драчков С.А., Павлушов Е.И.
126	ОАОИ	Мамонова Т.Ю., Кателкина С.В., Высоцкая А.И.
103	Бухгалтерия	Шиллер Н.М., Коротаева Т.Н., Чепрасова М.А., Курочкина В.Н., Пушкарева Л.А.
102	Бухгалтерия	Шиллер Н.М.
119	Отдел кадров	Петри Н.А.
201	Лечебный отдел	Райденко О.В.
202	Лечебный отдел	Коровина М.В.
206	Лечебный отдел	Журавлева Е.А.
207	Лечебный отдел	Свиридова Н.А.
209	Лечебный отдел	Шульженко Л.А.
210	Лечебный отдел	Новикова О.А.
211	Лечебный отдел	Кожевникова Е.Ю.
212	Лечебный отдел	Белоусова О.В.
213	Лечебный отдел	Галич Е.А.
214	Лечебный отдел	Маевская В.В.
215	Лечебный отдел	Ильина Е.А.
216	Лечебный отдел	Кузнецова Н.Н.
217	Лечебный отдел	Коваленко М.В.
135	Лечебный отдел	Садовая Н.В.
127	Лечебный отдел	Выродов И.В.

Ответственным лицам обеспечить расположение технических средств в ВП с учётом максимального затруднения визуального просмотра информации посторонними лицами, а также принимать дополнительные меры, исключающие подобный просмотр (шторы на окнах, жалюзи и т.п.)

Приложение 21

Перечень сведений ограниченного распространения

Информация, раскрывающая существо позиции представителей АКЦПБ со СПИДом по ведению судебных и арбитражных дел	1 год после прекращения ведения дела
Информация по делам, рассматриваемым в судах, разглашение которой может нанести ущерб интересам АКЦПБ со СПИДом	До даты вступления в силу судебного акта
Сведения о проведении АКЦПБ со СПИДом закрытых конкурсов, торгов и аукционов.	До даты извещения участников
Информация о привлечении консультантов, круге вопросов, которые им поручается исследовать, условия договоров с ними	1 год после исполнения договора, если иной срок не указан в договоре
Информация о проектах связанных с приобретением/отчуждением недвижимости (сведения об объекте, потенциальных приобретателях/отчуждателях, условия приобретения/отчуждения)	До момента государственной регистрации перехода права собственности; условия сделок 1 год после исполнения договора
Сведения о производственной, экономической и финансовой деятельности партнеров (контрагентах) АКЦПБ со СПИДом, с которыми осуществляется деловое сотрудничество, заключенное на условиях конфиденциальности	Определяется соглашением о конфиденциальности
Сведения о производственной, экономической и финансовой деятельности юридических лиц, полученные на условиях конфиденциальности	Постоянно
Сведения о выборе контрагентов для ведения коммерческих переговоров	До момента заключения договора
Условия договора (контрактов, соглашений) отнесенные исполнителем осуществляющим подготовку проекта договора к коммерческой тайне, или должностным лицом, подписывающим договор	На срок, установленный соглашением о конфиденциальности
Сведения о планируемых и проводимых режимных мероприятиях и их результатах	1 год
Сведения, раскрывающие организацию и состояние охраны объектов АКЦПБ со СПИДом (вооружение, техническое оснащение, численность, система охраны и связи, противодиверсионные и антитеррористические мероприятия и т.д.).	Постоянно
Сведения о применяемых методах и надежности защиты помещений, средств вычислительной техники, информационно-телекоммуникационных сетей и другого оборудования от утечки защищаемой информации, несанкционированных непреднамеренных воздействий на защищаемую информацию.	Постоянно
Сведения о проектных решениях по обеспечению защиты информации при разработке перспективных и модернизации существующих информационных систем, систем связи и передачи данных	Постоянно
Сведения о состоянии и мерах по совершенствованию си-	До формирования

стемы защиты конфиденциальной информации	новых систем
Сведения о результатах комплексных проверок состояния защиты информации	До формирования новых систем
Сведения о потенциальных каналах утечки информации	Постоянно
Отчетность, содержащая анализ состояния организационно-технических средств защиты информации, содержащей сведения, составляющие коммерческую тайну	Постоянно
Сведения об используемых сетевых адресах и паролях автоматизированных и информационно-управляющих систем производственной и финансово-экономической деятельности	Постоянно
Содержание базы данных и программного обеспечения цифровых автоматизированных телекоммуникационных систем, находящихся на узлах связи АКЦПБ со СПИДом	Постоянно
Сведения о способах и методах получения для АКЦПБ со СПИДом важной информации, в том числе при проверке установочных данных о лицах, принимаемых на должности в АКЦПБ со СПИДом	Постоянно
Систематизированные данные о лицах, получивших доступ конфиденциальной информации	Постоянно
Сведения о работниках АКЦПБ со СПИДом и информация об уровне доступа.	На период действия трудового договора и в течение 3-лет после его прекращения
Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.	На период действия трудового договора и в течение 3-лет после его прекращения
Сведения, ставшие известными в ходе исполнения своих должностных обязанностей.	Постоянно
Значения паролей, ключей, электронных цифровых подписей, применяемых в ЛВС АКЦПБ со СПИДом	Постоянно

Приложение 22

Инструкция по обращению с конфиденциальными носителями информации

1. Общие положения.

1.1. Инструкция по конфиденциальному делопроизводству в **АКЦПБ со СПИДом** (далее – Инструкция) устанавливает порядок и общие требования к организации работы с документами, содержащими конфиденциальную информацию. Требования Инструкции направлены на обеспечение мер по защите документированной содержащих информацию ограниченного доступа. Выполнение требований Инструкции обязательно для всех работников АКЦПБ со СПИДом, получивших доступ к такой информации.

1.2. Инструкция разработана в соответствии с законодательством Российской Федерации, и внутренними организационно-распорядительными документами.

1.3. Положения Инструкции распространяются на учреждение и технологию работы с конфиденциальными документами, независимо от вида носителя информации.

1.4. Ответственность за состояние конфиденциального делопроизводства в подразделениях несут их руководители.

Права и обязанности лиц, ответственных за ведение конфиденциального делопроизводства, закрепляются в их должностных инструкциях.

1.5. Для проведения ежегодных проверок наличия конфиденциальных документов, уничтожения носителей конфиденциальной информации, снятия грифов конфиденциальности с документов, расследования фактов утраты носителей конфиденциальной информации и разглашения, содержащихся в них сведений, перегруппировки конфиденциальных документов в делах. Распоряжением руководителя назначается Комиссия по вопросам конфиденциального делопроизводства (далее - Комиссия).

В Комиссию в обязательном порядке включаются работники, ответственные за ведение конфиденциального делопроизводства в АКЦПБ со СПИДом

2. Основные термины и определения.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Конфиденциальная информация АКМИАЦ определяется «Перечнем сведений ограниченного распространения».

Носители конфиденциальной информации – материальные объекты, в которых конфиденциальная информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Гриф конфиденциальности – реквизиты, свидетельствующие о конфиденциальности информации, содержащейся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Для служебного пользования(СП) — конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Конфиденциальный документ – документ, содержащий конфиденциальную информацию и имеющий гриф конфиденциальности.

Конфиденциальное делопроизводство – направление деятельности, обеспечивающее документирование и организацию работы с конфиденциальными документами;

Исполнитель документа – работник, осуществляющий подготовку проекта документа.

3. Подготовка, оформление документов и учет материальных носителей конфиденциальной информации.

3.1. Подготовка, оформление и согласование конфиденциальных документов осуществляется в соответствии с организационно-распорядительными документами (далее – ОРД), регламентирующими открытое делопроизводство в АКЦПБ со СПИДом, с учетом положений настоящей Инструкции. Все конфиденциальные документы подлежат однократной регистрации.

3.2. Конфиденциальная информация может содержаться на бумажных, электронных, магнитных и оптических носителях, в кино- и фотоматериалах.

3.3. На документах, содержащих конфиденциальную информацию АКЦПБ со СПИДом, исполнителем, его руководителем или лицом, подписывающим или утверждающим документ, проставляются грифы конфиденциальности с указанием полного наименования и места нахождения обладателя этой информации «Для служебного пользования» - на документах, содержащих информацию, составляющую служебную тайну, в соответствии с Перечнем сведений ограниченного распространения АКЦПБ со СПИДом, и иной конфиденциальной информации по форме, согласно Приложению № 1.

Электронные версии документов, содержащих конфиденциальную информацию, также должны иметь соответствующие грифы.

Также допускается проставление на материальных носителях конфиденциальной информации штампов с грифами конфиденциальности (*Приложение 23*).

3.4. Внешние электронные накопители (дискеты, CD-диски и другие накопители), используемые для хранения конфиденциальной информации, подлежат учету в Журнале учета внешних электронных и других накопителей, используемых для хранения конфиденциальной информации (*Приложение 24*). При хранении конфиденциальной информации на дискетах грифы «Для служебного пользования» и учетный номер носителя информации указываются на бумажной наклейке дискеты. Указанные реквизиты должны быть нанесены также на CD-диски и другие внешние электронные накопители, используемые для хранения конфиденциальной информации. Гриф конфиденциальности и учетный номер носителя наносятся специальным маркером либо иным доступным способом.

Учетный номер электронного носителя конфиденциальной информации состоит из номера Журнала учета внешних электронных и других накопителей, буквенного обозначения «СП» и порядкового номера по Журналу учета внешних электронных и других накопителей.

Для обозначения конфиденциальной информации, размещенной на аудио, видео, кино- и фотоматериалах, используются буквы «СП».

Запрещается записывать на внешние электронные накопители, имеющие грифы «Для служебного пользования, файлы, не содержащие конфиденциальной информации.

3.5. Гриф проставляется без кавычек в правом верхнем углу первой страницы документа, на титульном листе, а также на первой странице сопроводительного письма к конфиденциальным материалам.

На документе ниже грифа конфиденциальности указывается номер экземпляра (*Приложение 23*)

3.6. Черновики конфиденциальных документов уничтожаются (измельчаются механическим способом до степени, исключающей возможность прочтения текста) исполнителем.

3.7. Решение вопроса о снятии грифа конфиденциальности с документа, в том числе в связи с истечением срока действия режима конфиденциальности в отношении содержащихся в документе сведений, возлагается на Комиссию, созданную в АКЦПБ со СПИДом (*Приложение 25*). Заключение Комиссии оформляется Актом (*Приложение 26*), утвержда-

емым руководителем учреждения. При этом на документе делается письменная отметка о снятии грифа:

«Гриф снят. Акт №___ от _____ (дата)», заверенная подписью лица, ответственного за ведение конфиденциального делопроизводства, и круглой печатью. Аналогичные отметки вносятся в описи дел. Документы со снятыми грифами конфиденциальности из дел изымаются.

4. Работа с входящей, исходящей и внутренней конфиденциальной корреспонденцией.

4.1. Работа с входящей, исходящей и внутренней конфиденциальной корреспонденцией в АКЦПБ со СПИДом организуется в соответствии с требованиями ОРД, регламентирующих открытое делопроизводство, с учетом положений настоящей Инструкции.

4.2. Особенности при работе с конфиденциальной корреспонденцией:

4.2.1. Сканирование конфиденциальных документов запрещается.

4.2.2. Конверты (пакеты) с грифом конфиденциальности, поступившие в управление, вскрываются, (кроме указанных в п. 4.2.4). При этом проверяется правильность адресации, целостность упаковки документов и комплектность (при наличии описи или перечисления в сопроводительном документе либо на конверте).

Неправильно адресованные, ошибочно вложенные документы пересылаются по назначению или возвращаются отправителю.

При обнаружении недостачи документов или приложений к ним составляется акт в трех экземплярах, один из которых остается в секретариате, второй приобщается к поступившему документу, третий посылается отправителю (в соответствии с ОРД, регламентирующими открытое делопроизводство).

Каждый документ с грифом конфиденциальности, поступивший в секретариат, регистрируется рукописным способом в Журнале регистрации входящих конфиденциальных документов (*Приложение 27*).

4.2.3. Если документ адресован напрямую в подразделение АКЦПБ со СПИДом, то он передается под роспись в Журнале регистрации входящих конфиденциальных документов ответственному за ведение конфиденциального делопроизводства в данном подразделении для представления его руководителю, последующего изучения, исполнения и реализации. При этом ответственный за ведение конфиденциального делопроизводства данного подразделения регистрирует документ в своем Журнале регистрации входящих конфиденциальных документов, и после резолюции руководителя передает на исполнение работнику под роспись в указанном Журнале.

4.2.4. Поступивший документ с грифом конфиденциальности на имя руководителя после внесения в Журнал регистрации входящих конфиденциальных документов передается ему для рассмотрения. После наложения резолюции для исполнения данный документ передается в подразделение с выполнением всех требований п. 4.2.3.

4.2.5. Конверты (пакеты) с грифом «Для служебного пользования» или «Конфиденциально», содержащие дополнительную отметку «Лично», регистрируются и передаются непосредственно адресату под роспись в Журнале регистрации входящих конфиденциальных документов. Конверты (пакеты) вскрываются лично адресатом, на первый лист документа переносится номер и дата регистрации конверта (пакета). Записи о решениях об исполнении таких документов осуществляются по поручению адресата лицом, ответственным за ведение конфиденциального делопроизводства в АКЦПБ со СПИДом или подразделении.

4.2.6. Поступившие в подразделения конфиденциальные документы подлежат обязательному учету в Журналах регистрации входящих конфиденциальных документов (*Приложение 27*) работниками, ответственными за ведение конфиденциального делопроизводства в подразделениях. Входящий номер конфиденциального документа состоит из номе-

ра Журнала регистрации входящих конфиденциальных документов, буквенного обозначения «СТ» и порядкового номера в Журнале регистрации входящих конфиденциальных документов в пределах календарного года, например: вх. № 1/СТ-124.

При любых движениях документа в подразделениях за ним остается только тот учетный номер, который был ему присвоен при первичной регистрации в подразделении, когда он поступил в организацию.

Документы, адресованные от внешних отправителей, доставленные нарочным подлежат вскрытию (пакеты), проверке и регистрации в секретариате (согласно п. 4.2.2).

Документы учитываются по количеству листов, издания – поэкземплярно (в графе 8 Журнала), а дискеты, CD-диски и другие внешние электронные накопители, аудио- и видеокассеты – поштучно.

4.2.7. Отправляемые документы, содержащие конфиденциальную информацию, подписанные руководителем, его заместителями, руководителями подразделений и иными лицами, уполномоченными правом подписи исходящей корреспонденции, регистрируются в установленном порядке в Журнале регистрации исходящих конфиденциальных документов секретариата (*Приложение 28*). При регистрации в Журнале номер исходящего документа дополняется буквенным обозначением («СП»). После регистрации документы передаются для отправки.

4.2.8. Отправляемые документы, содержащие конфиденциальную информацию, адресованные органам государственной власти или организациям, после регистрации оформляются к отправке в конвертах. В правом углу конверта проставляется гриф «Для служебного пользования» (отступив 3-4 см от верхней кромки). В левом нижнем углу конверта обязательно указывается номер документа (номера документов), вложенного в конверт.

4.3. Все виды Журналов, предназначенные для учета документов, содержащих конфиденциальную информацию, должны быть прошнурованы и все страницы пронумерованы. На последней странице Журнала цифрами и прописью указывается количество содержащихся в нем листов, которое заверяется подписью работника, ответственного за ведение конфиденциального делопроизводства в АКЦПБ со СПИДом (отделе; подразделении) и круглой печатью. Регистрация документов в таких Журналах ежегодно начинается с первого номера, а по окончании года делается итоговая запись о количестве документов.

Журналы заполняются аккуратным, разборчивым почерком с расшифровкой подписей всех лиц, кому был передан документ. Все исправления в Журналах заверяются подписью работника, ответственного за ведение конфиденциального делопроизводства.

5. Группировка конфиденциальных документов в дела.

5.1. Порядок группировки конфиденциальных документов в дела определяется ОРД, регламентирующими открытое делопроизводство в АКЦПБ со СПИДом, с учетом положений настоящей Инструкции.

5.2. В номенклатуру дел АКЦПБ со СПИДом в обязательном порядке включаются дела с грифом «Для служебного пользования», а также журналы учета конфиденциальных документов. В данной номенклатуре дел подразделений при ограниченном объеме хранимых документов допускается подшивать их в одно дело. Срок хранения дел в номенклатуре дел указывается по максимальному сроку хранения содержащихся в них документов.

5.3. После исполнения документы подшиваются в дело. Конфиденциальные документы группируются в дела отдельно от документов открытого характера.

5.4. Делу с конфиденциальными документами присваивается гриф конфиденциальности. В номенклатуре дел в графе «Индекс дела» к номеру дела добавляется отметка «СП».

5.5. Дата начала дела должна соответствовать дате первого подшитого в дело конфиденциального документа, подшитого в нем. Эта дата проставляется на обложке дела после того, как в него будет подшит последний документ

5.6. Все подшитые в дело (том) конфиденциальные документы нумеруются полистно, номера проставляются простым карандашом в правом верхнем углу листа документа. На все подшитые конфиденциальные документы составляется внутренняя опись (*Приложение 29*), которая заполняется по мере подшивки в дело документов.

Листы внутренней описи дела нумеруются отдельно. Листы ознакомления с распорядительными конфиденциальными документами подшиваются в дела вместе с этими документами, вносятся во внутреннюю опись и нумеруются.

По окончании дела (тома) в конце внутренней описи указывается должность и фамилия работника, ответственного за ведение конфиденциального делопроизводства.

5.7. Законченное дело (том) с документами прошивается, опечатывается и заверяется работником, ответственным за ведение конфиденциального делопроизводства в АКЦПБ со СПИДом (отделе, подразделении). Опечатывание дела (тома) производится с помощью бумажной наклейки, которая наклеивается так, чтобы захватывались нити шнурка прошивки дела (тома), и заверяется оттиском круглой печати. Опечатанные дела переплету не подлежат.

5.8. Во внутренней описи переходящего дела, после ежегодной проверки наличия документов Комиссией, делается итоговая запись о количестве подшитых в деле листов по состоянию на 31 декабря каждого года, которая заверяется подписью председателя Комиссии. Нумерация листов переходящего дела после итоговой записи продолжается от номера последнего листа прошлого года.

5.9. По окончании делопроизводственного года дело с грифом «Для служебного пользования» просматривается полистно Комиссией и, в случае необходимости, принимается решение о перегруппировке документов.

Содержащиеся в этом деле документы, имеющие срок постоянного хранения (либо их постоянное хранение вызвано служебной необходимостью), группируются в отдельное дело (дела), которое получает самостоятельный заголовок и дополнительно включается в номенклатуру дел.

Если в дело включены документы только временных сроков хранения, оно может не переформировываться. Срок хранения такого дела устанавливается по максимальному сроку хранения содержащихся в нем документов.

5.10. После снятия конфиденциальности документ может быть перемещен в соответствующее дело открытого делопроизводства, о чем делается соответствующая отметка в описи дела.

5.11. Конфиденциальные дела, хранящиеся в АКЦПБ со СПИДом, выдаются ответственными за ведение конфиденциального делопроизводства только тем исполнителям, которые имеют к ним прямое отношение для исполнения своих служебных обязанностей.

5.12. Подготовка дел для архивного хранения и передача в архив производятся в соответствии с ОРД, регламентирующими открытое делопроизводство в АКЦПБ со СПИДом.

Дела передаются в архив АКЦПБ со СПИДом с обязательной полистной проверкой включенных в них документов.

5.13. При необходимости изъятия из дела документа, содержащего информацию, составляющую служебную тайну АКЦПБ со СПИДом, дело расшивается, документ изымается. В протоколе выемки должны быть указаны гриф конфиденциальности, учетный номер и номер экземпляра изымаемого документа и ссылка на должностное лицо, по указанию которого произведена выемка документа и причина выемки. Протокол выемки подшивается в дело вместо изъятого документа.

6. Хранение и использование конфиденциальных документов.

6.1. Документы, дела и другие конфиденциальные материалы должны храниться в служебных помещениях и (или) архивах АКЦПБ со СПИДом в запираемых шкафах и сейфах.

6.2. За сохранность конкретного конфиденциального документа отвечает работник, получивший этот документ в пользование.

6.3. При смене или увольнении работника, ответственного за ведение конфиденциального делопроизводства, составляется Акт приема-передачи этих документов (*Приложение 30*), утверждаемый руководителем АКЦПБ со СПИДом.

6.4. Запрещается выносить документы, дела и другие конфиденциальные материалы из служебных помещений для работы с ними на дому, в гостинице и т.д. В необходимых случаях руководитель АКЦПБ со СПИДом, подразделения может разрешить исполнителям или другим работникам вынос из здания конфиденциальных документов для их согласования, подписи и т.п. в других организациях. Работникам, командируемым за пределы г.Барнаула, по письменной резолюции их руководителя разрешается иметь при себе в пути следования конфиденциальные материалы.

6.5. О фактах утраты конфиденциальных документов, дел и других материалов, либо разглашения содержащихся в них сведений немедленно ставятся в известность непосредственный руководитель, ответственный за организацию режима защиты информации в АКЦПБ со СПИДом.

По факту утраты конфиденциальных документов, дел и других материалов или разглашения сведений, содержащихся в этих материалах, Комиссией проводится служебное расследование. В данном случае в состав Комиссии включается работник отдела сетевых технологий и защиты информации. По результатам работы Комиссии составляется Акт. Соответствующие отметки вносятся в учетные документы.

7. Тиражирование конфиденциальных документов.

Для копирования, размножения конфиденциальных документов исполнитель обязан использовать технику, исключающую возможность получения повторных несанкционированных копий документов (электронных документов), либо убедиться в невозможности дальнейшего получения таких копий.

8. Пересылка конфиденциальных документов.

8.1. Пересылка материалов с конфиденциальной информацией в другие организации производится заказными почтовыми отправлениями, курьерской службой, фельдъегерской связью, спецсвязью или нарочными.

8.2. Запрещается передавать конфиденциальные документы по незащищенным каналам связи: с использованием факсимильной связи, сетей Интернет, Интранет, и т.п., без принятия достаточных мер по защите информации.

8.3. При пересылке конфиденциальных документов в Журнале регистрации исходящих конфиденциальных документов в графе «Примечание» указывается способ отправки.

8.4. При направлении конфиденциальных документов в несколько адресов составляется список рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Список рассылки подписывается исполнителем и утверждается руководителем организации.

9. Уничтожение конфиденциальных документов.

9.1. Выделение к уничтожению и уничтожение носителей конфиденциальной информации, утративших свою актуальность и необходимость дальнейшего их хранения, производится Комиссией АКЦПБ со СПИДом.

9.2. Выделенные к уничтожению бумажные носители конфиденциальной информации измельчаются механическим способом до степени, исключающей возможность прочтения текста в присутствии вышеуказанной Комиссии.

9.3. Конфиденциальная информация, хранящаяся на магнитных носителях, производится путем ее стирания с использованием специальных средств.

9.4. Факт уничтожения конфиденциальных материалов оформляется соответствующим актом в двух экземплярах (*Приложение 30*).

9.5. После уничтожения материалов в Журналах регистрации конфиденциальных документов и изданий, в номенклатурах и описях дел, а также в Журналах учета внешних электронных и других накопителей конфиденциальной информации проставляется отметка

«Уничтожено. Акт № ___ от _____».

10. Контроль состояния конфиденциального делопроизводства.

10.1. По окончании года в отделах и подразделениях АКЦПБ со СПИДом, Комиссией проводится проверка наличия конфиденциальных документов. Основанием для проверки может стать перемещение документов, ликвидация подразделения, чрезвычайные ситуации и т.д.

Комиссия проверяет выполнение требований настоящей Инструкции, наличие текущих дел и дел с временными сроками хранения, наличие конфиденциальных документов, не подшитых в дела. Проверка наличия документов производится путем сверки Журналов учета с фактическим наличием документов, а также отметок об уничтожении или отправке документов в этих Журналах с Актами и Реестрами.

В Журналах учета, переходящих из года в год, все произведенные отметки об отправке, уничтожении и переучете конфиденциальных документов заверяются проставлением записи «Проверено» с датой и подписью председателя Комиссии.

10.2. К началу работы Комиссии все исполненные конфиденциальные документы, должны быть учтены в конфиденциальном делопроизводстве, приобщены к делам или перерегистрированы в Журналах учета нового года, в старых производится отметка об их перерегистрации в указанием новых учетных номеров.

10.3. По результатам работы Комиссии составляется Акт проверки (*Приложение 32*), который утверждается руководителем АКЦПБ со СПИДом. В Акте указываются результаты проверки конфиденциального делопроизводства, отмеченные недостатки и предложения по улучшению состояния дел по вопросам защиты конфиденциальной информации.

Приложение 23
к Инструкции по конфиденциальному
делопроизводству

Для служебного пользования
Экз. № 1.

АКЦПБ со СПИДом
СЛУЖЕБНАЯ ЗАПИСКА
«_____»_____200__г. №_____

Образец

Уч. № … *(№ по Журналу учета проектов документов на бумажных носителях конфиденциальной информации)*

(оборотная сторона)

Приложение 24
к Инструкции по конфиденциальному
делопроизводству

АКЦПБ со СПИДом

Журнал учета внешних электронных и других накопителей,
используемых для хранения конфиденциальной информации.

Уч. №	Тип носи-теля	Объем памяти, МБ	Кому выдано (Ф.И.О.) или куда направлено	Расписка в получении или номер исходящего документа	Отметка о возврате (Ф.И.О. ответствен-ного лица, расписка и дата)	Отметка об уни-чтожении (Ф.И.О. ответственного ли-ца, расписка и дата)
1.	2.	3.	4.	5.	6.	7.

Приложение 25
к Инструкции по конфиденциальному
делопроизводству

УТВЕРЖДАЮ

«____»_____ 200 __ г.

Состав комиссии по снятии грифа конфиденциальности с документа

Председатель комиссии: Хаустова Л.В.

Члены комиссии:

Белоусова О.В.
Попова В.В.
Домашец А.М.

Приложение 26
к Инструкции по конфиденциальному
делопроизводству

УТВЕРЖДАЮ

«____»_____ 200 __ г.

АКЦПБ со СПИДом

АКТ
о снятии грифов конфиденциальности с документов

«____»_____ 200 _ г. № _____

№ п/п	Номер и дата документа, индекс дела, куда был подшит документ	Заголовок документа, гриф конфиденциальности	Кол-во листов	Причина снятия грифа	Индекс дела, куда будет подшит документ
1.	2.	3.	4.	5.	6.

Председатель комиссии: _____
(должность, подпись, фамилия, инициалы)

Члены комиссии: _____
(должность, подпись, фамилия, инициалы)

_____
(должность, подпись, фамилия, инициалы)

_____
(должность, подпись, фамилия, инициалы)

Приложение 27
к Инструкции по конфиденциальному
делопроизводству

АКЦПБ со СПИДом

Журнал регистрации входящих конфиденциальных документов.

№ п/п	Входящий номер и дата поступления	Дата и исходящий номер документа, присвоенный отправителем	Откуда поступил	Наименование документа и краткое содержание (тема документа)	Количество листов (изданий)		Количество и номера экземпляров
					документа	приложения	
1.	2.	3.	4.	5.	6.	7.	8.

Резолюция или кому направлен на исполнение	Отметка о взятии на контроль и срок исполнения	Дата и расписка		Номер дела, куда подшит документ	Отметка об уничтожении	Примечание
		в получении	в возврате			
9.	10.	11.	12.	13.	14.	15.

Приложение 28
к Инструкции по конфиденциальному делопроизводству

АКЦПБ со СПИДом

Журнал регистрации исходящих конфиденциальных документов.

№ п/п	Регистрационный номер и дата документа	Куда направлен	Наименование документа и краткое содержание (тема документа)	Количество листов	
				документа	приложения
1.	2.	3.	4.	5.	6.

Количество и номера экземпляров	Исполнитель	Дата и расписка		Индекс (номер) дела, куда подшит документ	Отметка об уничтожении	Примечание
		в получении	в возврате			
7.	8.	9.	10.	11.	12.	13.

Приложение 29
к Инструкции по конфиденциальному
делопроизводству

ВНУТРЕННЯЯ ОПИСЬ
документов, находящихся в деле № _____
том № _____ за 200__год

№ п/п	Номер документа	Дата документа	Заголовок документа	Номера листов	Примечание

Итого _____ документов
(цифрами и прописью)

Количество листов внутренней описи _____.
(цифрами и прописью)

Наименование должности лица,
составившего внутреннюю опись
документов дела Подпись Фамилия, инициалы

Дата

Приложение 30
к Инструкции по конфиденциальному
делопроизводству

УТВЕРЖДАЮ

«____»_____ 200 __ г.

АКЦПБ со СПИДом

АКТ
приема-передачи документов (дел) с грифом
«Для служебного пользования»

«____»_____ 200 _ г. № _____

№ п/п	Номер и дата документа (индекс и крайние даты дела)	Заголовок документа (дела)	Количество листов документа (дела)
1.	2.	3.	4.

Всего _____ документов (дел)
(количество документов цифрами и прописью)

Передал _____
(должность, подпись, фамилия, инициалы)

Принял _____
(должность, подпись, фамилия, инициалы)

Приложение 31
к Инструкции по конфиденциальному
делопроизводству

УТВЕРЖДАЮ

«____»_____ 200 __ г.

АКЦПБ со СПИДом

АКТ
о выделении к уничтожению документов с грифом «Для служебного пользования», не подлежащих хранению

«____»_____ 200 _ г. № _____

На основании _____
Отобраны к уничтожению как не имеющие научно-исторической ценности и утратившие практическое значение следующие документы:

№ п/п	Заголовок документа	Дата документа	Номер документа по журналу	Срок хранения	Примечание
1.	2.	3.	4.	5.	6.

Документы уничтожены путем _____.

Председатель комиссии: _____
(подпись) (Должность, фамилия, инициалы)

Члены комиссии: _____
(подпись) (Должность, фамилия, инициалы)

_____
(подпись) (Должность, фамилия, инициалы)

Приложение 32
к Инструкции по конфиденциальному
делопроизводству

УТВЕРЖДАЮ

«____»_____ 200 __ г.

АКЦПБ со СПИДом

АКТ
проверки наличия и состояния документов и дел с грифом
«Для служебного пользования»

«____»_____ 200 _ г. № _____

Основание:_____
(плановая проверка, перемещение документов, стихийное бедствие и т.д.)

Проверкой установлено:
I. Всего числится по описям (номенклатурам дел, журналам учета)
_____ (документов, дел)
(цифрами и прописью)

1) из них имеется в наличии_____
2) не обнаружено_____
(индексы (номера) документов, дел, изданий)

II. Обнаружено не внесенных в описи (номенклатуры дел, журналы учета)
_____

III. Характеристика состояния документов, дел и изданий
_____

Решение по результатам проверки:
_____

Председатель комиссии: _____
(подпись)
(Должность, фамилия, инициалы)

Члены комиссии: _____
(подпись)
(Должность, фамилия, инициалы)

_____
(подпись)
(Должность, фамилия, инициалы)

_____
(подпись)

С приказом ознакомлены:
Алёхина Л.Н.
Анисимова А.С.
Белоусова О.В.
Высоцкая А.И.
Выродов И.В.
Выходцев С.Н.
Галич Е.А.
Глумова А.Е.
Демьяненко Э.Р.
Домашец А.М.
Драчков С.А.
Дюканова О.И.
Ильина Е.А.
Журавлева Е.А.
Коваленко М.В.
Кожевникова Е.Ю.
Коломоец Ю.П.
Коротаева Т.Н.
Кателкина С.В.
Коровина М.А.
Коломоец Ю.П.
Кузнецова Н.Н.
Курочкина В.Н.
Лукьянова В.А.
Маевская В.В.
Мамонова Т.Ю.
Минакова М.В.
Николенко А.А.
Новикова О.А.
Павлушов Е.И.
Петри Н.А.
Попова В.В.
Поподьина Е.Б.
Пушкарева Л.А.
Райденко О.В.
Садовая Н.В.
Свиридова Н.А.
Торовкова Т.В.
Хаустова Л.В.
Чепрасова М.А.
Цветкова А.Г.
Шиллер Н.М.
Шульженко Л.А.
Щербинина Ю.О.