БАШКОРТОСТАН РЕСПУБЛИКАҺЫ
ҺАУЛЫҚ ҺАҡЛАУ МИНИСТРЛЫҒЫ

БАШКОРТОСТАН РЕСПУБЛИКАҺЫ
ДӘҮЛӘТ БЮДЖЕТ ҺАУЛЫҚ
ҺАҡЛАУ УЧРЕЖДЕНИЕҺЫ
БАҡАЛЫ ҮЗӘК
РАЙОН ДАУАХАНАҺЫ
(РБ ДБҺҺУ Бакалы УРД)

452650, Башкортостан Республикаһы, Бакалы районы,
Бакалы ауылы, Шакирйанов ур., 2
Тел./факс 8 (34742) 3-22-60
E-mail: BAKAL.CRB@doctorrb.ru

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ БАШКОРТОСТАН

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ БАШКОРТОСТАН
БАКАЛИНСКАЯ ЦЕНТРАЛЬНАЯ
РАЙОННАЯ БОЛЬНИЦА
(ГБУЗ РБ Бакалинская ЦРБ)

452650, Республика Башкортостан, Бакалинский
район, с. Бакалы, ул. Шакирьянова, 2
Тел./факс 8 (34742) 3-22-60
E-mail: BAKAL.CRB@doctorrb.ru

П Р И К А З

«09»__01___2023 г. **№ 113**

«О назначении ответственных лиц за организацию обработки персональных данных»

На основании Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», в соответствии с Постановлением Правительства РФ от 21.03.2012г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»,

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке персональных данных пациентов в ГБУЗ РБ Бакалинская ЦРБ (Приложение № 1)
2. Утвердить Политику обработки персональных данных в ГБУЗ РБ Бакалинская ЦРБ (Приложение № 2)
3. Утвердить перечень персональных данных, обрабатываемых в ГБУЗ РБ Бакалинская ЦРБ, в связи с реализацией трудовых отношений (Приложение № 3).
4. Утвердить перечень должностей ГБУЗ РБ Бакалинская ЦРБ ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных (Приложение № 4).
5. Утвердить перечень персональных данных, обрабатываемых в ГБУЗ РБ Бакалинская ЦРБ в связи с осуществлением медицинской деятельности (Приложение № 5).
6. Утвердить перечень информационных систем персональных данных ГБУЗ РБ Бакалинская ЦРБ (Приложение № 6).
7. Утвердить перечень мест хранения персональных данных (Приложение № 7).
8. Утвердить модель угроз безопасности персональных данных при обработке в информационной системе персональных данных ГБУЗ РБ Бакалинская ЦРБ (Приложение № 8).

9. Утвердить матрицу доступа сотрудников к информационным ресурсам информационных систем ГБУЗ РБ Бакалинская ЦРБ (Приложение № 9).

10. Утвердить правила работы с обезличенными персональными данными в ГБУЗ РБ Бакалинская ЦРБ (Приложение № 10).

11. Утвердить типовое обязательство сотрудника ГБУЗ РБ Бакалинская ЦРБ непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора, о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей (Приложение № 11).

12. Утвердить парольную политику в отношении к Государственной информационной системы «Региональная информационно-аналитическая система Республики Башкортостан» (ГИС «РМИАС РБ») (Приложение № 12)

13. Самигуллину Т.Х. – заместителя главного врача по медицинской части назначить ответственной за организацию обработки персональных данных по лечебно-профилактическому учреждению.

14. Закирову Э.М. – начальника отдела кадров назначить ответственной за организацию обработки персональных данных в связи с реализацией трудовых отношений.

15. Павлова И.С. – заведующего отделением первичной специализированной медико-санитарной помощи назначить ответственным за организацию обработки персональных данных по поликлинике.

16. Ахатову Л.А. – заведующего кабинета медицинской статистики назначить ответственной за организацию обработки персональных данных по стационару.

17. Таджибаеву М.Н. – программисту:

17.1. Ежегодно проверять наличие сведений на сайте http://pd.rsoc.ru/operators-registry/ operators-list/;

17.2. При обработке персональных данных в информационных системах принимать необходимые технические меры.

18. Хабировой З.М.- делопроизводителю ознакомить с приказом под роспись.

19. Контроль за исполнением данного приказа оставляю за собой.

Главный врач
ГБУЗ РБ Бакалинская ЦРБ З.С. Гиздатуллин

Приложение № 1
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

ПОЛОЖЕНИЕ
об обработке персональных данных пациентов в Государственном бюджетном учреждении здравоохранения Республики Башкортостан Бакалинская центральная районная больница

1. Общие положения.

1.1.Согласно ст. 23 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную, семейную тайну, защиту своей чести и доброго имени, реализация которого обеспечивается положением ст. 24 Конституции РФ, устанавливающим, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается. В соответствии с законодательством Российской Федерации информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных действующим законодательством. Отношения, связанные с обработкой персональных данных, осуществляемой юридическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, регулируются

Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

Настоящее Положение разработано в целях выполнения указанных выше норм Конституции РФ, в соответствии с требованиями законодательства Российской Федерации и иных нормативных правовых актов в сфере охраны здоровья населения и обработки персональных данных.

1.2.Настоящее Положение определяет порядок работы (получения, обработки, использования, передачи, хранения и т.д.) сотрудников ГБУЗ РБ Бакалинская ЦРБ (далее Оператор) с персональными данными пациентов и гарантии конфиденциальности сведений о пациенте, предоставленных пациентом в ГБУЗ РБ Бакалинская ЦРБ; права пациента при обработке его персональных данных; ответственность лиц за невыполнение требований норм, регулирующих обработку персональных данных пациента.

2. Понятие и состав персональных данных пациента

2.1.Персональные данные пациента - любая информация, относящаяся к прямо или косвенно к пациенту (субъекту персональных данных).

2.2.В целях ведения персонифицированного учета осуществляется

обработка следующих персональных данных о лицах, которым оказываются медицинские услуги (пациентах):

1) фамилия, имя, отчество (последнее - при наличии);
2) пол;
3) дата рождения;
4) место рождения;
5) гражданство;
6) данные документа, удостоверяющего личность;
7) место жительства;
8) место регистрации;
9) дата регистрации;
10) страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
11) номер полиса обязательного медицинского страхования застрахованного лица (при наличии);
12) анамнез;
13) диагноз;
14) сведения об организации, оказавшей медицинские услуги;
15) вид оказанной медицинской помощи;
16) условия оказания медицинской помощи;
17) сроки оказания медицинской помощи;
18) объем оказанной медицинской помощи;
19) результат обращения за медицинской помощью;
20) серия и номер выданного листка нетрудоспособности (при наличии);
21) сведения об оказанных медицинских услугах;
22) примененные порядки и стандарты медицинской помощи;
23) сведения о медицинском работнике или медицинских работниках, оказавших медицинскую услугу.

Все персональные данные, касающиеся состояния здоровья пациента, относятся к специальным категориям персональных данных и обрабатываются в соответствии с установленным законодательством и иными нормативными правовыми актами требованиями.

3. Сбор, цели обработки и защита персональных данных пациента

3.1.Обработка персональных данных осуществляется:

- после получения письменного согласия субъекта персональных данных, составленного по утверждённой Оператором форме, соответствующей требованиям федерального закона, за исключением случаев, предусмотренных частью 2 статьи 6 ФЗ «О персональных данных»;
- после направления уведомления об обработке персональных данных в орган государственного надзора в сфере связи, информационных технологий и массовых коммуникаций территории, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона «О персональных данных»;
- после принятия Оператором необходимых мер по защите

персональных данных.

3.2.Все персональные данные пациента следует получать лично у пациента или у его законного представителя. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

3.3.Оператор сообщает пациенту или его законному представителю о целях обработки персональных данных, предполагаемых источниках и способах получения персональных данных и последствиях отказа пациента дать письменное согласие на их получение.

3.4.Оператор осуществляет обработку персональных данных только после получения письменного согласия пациента (или его законного представителя) на обработку его персональных данных за исключением случаев, предусмотренных действующим законодательством.

3.5.При обращении за медицинской помощью пациент (или его законный представитель) предоставляет Оператору персональные данные о себе в документированной форме. А именно:

- паспорт или иной документ, удостоверяющий личность;
- полис обязательного медицинского страхования;
- направление (при наличии).

При отсутствии документов пациент (или его законный представитель) предоставляют Оператору необходимые персональные данные в устной форме.

3.6.Оператор с согласия пациента может запрашивать и получать персональные данные пациента, используя информационные системы персональных данных с применением средств автоматизации.

3.7.Обработка Оператором персональных данных пациента осуществляется исключительно в целях оказания пациенту качественной медицинской помощи в необходимых объёмах, соблюдения требований действующего законодательства, иных нормативных правовых актов, обеспечения контроля объёмов и качества оказанной медицинской помощи.

3.8.Оператор при определении объема и содержания обрабатываемых персональных данных пациента руководствуется

Конституцией Российской Федерации, Основами законодательства Российской Федерации об охране здоровья граждан, иными нормативными правовыми актами в сфере охраны здоровья населения и обработки персональных данных.

3.9.Защита персональных данных пациента от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств в порядке, установленном законодательством, и принятыми Оператором в соответствии с ним локальными нормативными актами.

4. Порядок использования, хранения, передачи персональных данных пациента

4.1.Персональные данные пациентов предоставляются Оператору после получения соответствующего информированного согласия пациентов на обработку их персональных данных. Персональные данные пациентов у Оператора содержаться в информационных системах персональных данных,

представляющих собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. В информационных системах персональные данные могут быть размещены на материальных, в том числе бумажных носителях (медицинская карта пациента, иные медицинские документы).

4.2.Доступ к обработке персональных данных пациентов (как с использованием средств автоматизации, так и без использования средств автоматизации) обеспечивается в установленном Оператором порядке.

4.3.Конкретные обязанности по работе с информационными системами персональных данных и материальными носителями информации, в том числе с медицинскими документами, содержащими персональные данные пациентов возлагаются на сотрудников Оператора и закрепляются в должностных инструкциях.

4.4.Работа с информационными системами персональных данных, материальными носителями, в том числе с медицинской документацией, содержащими персональные данные пациентов осуществляется в специально отведённых для этого помещениях: ординаторские, кабинеты врачей, орг.- метод. отдел, кабинет медицинской статистики, регистратура, серверная и т.д.

4.5.Требования к месту обработки персональных данных, в том числе к серверной, обеспечивающие их защищённость устанавливаются Оператором.

4.6.Перечень лиц, имеющих право доступа к персональным данным пациентов и обработке их персональных данных, определяется приказом руководителя Оператора.

4.7.С лицами, допущенными к обработке персональных данных пациентов, заключается Соглашение о неразглашении.

4.8.Лица, допущенные в установленном порядке к обработке персональных данных, имеют право обрабатывать только те персональные данные пациентов, которые необходимы для выполнения конкретных функций.

4.9.Оператор при создании и эксплуатации информационных систем персональных данных пациентов с использованием средств автоматизации обеспечивает проведение классификации информационных систем (определение уровня защищенности) в установленном порядке.

4.10.Оператор при создании и эксплуатации информационных систем персональных данных пациентов с использованием средств автоматизации и без использования средств автоматизации принимает все необходимые организационные и технические меры, обеспечивающих выполнение установленных действующим законодательством требований к обработке персональных данных.

4.11.Оператор при осуществлении обработки персональных данных пациентов без использования средств автоматизации выполняет следующие требования.

4.11.1. При ведении журналов (реестров, книг, иных документов), содержащих персональные данные пациентов, необходимые для организации оказания медицинской помощи, Оператор соблюдает следующие условия:

– необходимость ведения такого журнала (реестра, книги, иных документов) предусматривается приказом Оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги, иных документов), сроки обработки персональных данных;

– копирование содержащейся в таких журналах (реестрах, книгах, иных документах) информации не допускается, за исключением случаев, предусмотренных действующим законодательством.

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

4.11.3. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

4.11.4. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

4.11.5. Уточнение персональных данных пациента при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

4.12. С согласия пациента или его законного представителя допускается передача сведений, в том числе персональных данных, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в интересах обследования и лечения пациента, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях.

4.13. Передача персональных данных пациента, составляющих врачебную тайну, без согласия пациента или его законного представителя допускается может допускается в случаях, предусмотренных частью 4 статьи 13 Федерального закона Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее Основы):

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 статьи 20 Основ;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Основ, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Основ, для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебнолетных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Основами.

4.14. При передаче персональных данных пациента сотрудники медицинской организации должны соблюдать следующие требования:

– не сообщать персональные данные пациента третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом;

– не сообщать персональные данные пациента в коммерческих и иных целях без его письменного согласия;

– предупредить лиц, получающих персональные данные пациента, 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 пациента, обязаны соблюдать режим секретности (конфиденциальности);

– разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, определенным приказом Руководителя, при этом указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных должностных функций;

– передавать персональные данные пациента представителям пациента в порядке, установленном законодательством, и ограничивать эту информацию только теми персональными данными пациента, которые необходимы для выполнения указанными представителями их функций.

4.15. 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.

4.16. Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими и фармацевтическими работниками с учетом причиненного гражданину ущерба несут за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации.

5. Права пациентов при обработке Оператором персональных данных пациентов

5.1.В целях обеспечения защиты своих интересов, реализации прав и свобод в сфере персональных данных, регламентированных действующим законодательством пациенты, их законные представители, а также представители имеют право на:

- предоставление Оператором полной информации об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные пациента, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- требование уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные пациента, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование действий или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Права пациента, представителя, законного представителя на доступ к своим персональным данным ограничиваются в случаях, предусмотренных действующим законодательством.

6. *Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных пациентов*

6.1 Лица, виновные в нарушении установленных требований в сфере обработки персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

6.2.Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, законодательством, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

6.3.Сотрудники Оператора, получившие в установленном порядке доступ к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных обучающихся привлекаются к ответственности, предусмотренной действующим законодательством.

7. *Заключительные положения*

Настоящее Положение вступает в законную силу с момента утверждения его руководителем Оператора и действует до утверждения нового положения.

Приложение № 2
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

ПОЛИТИКА
обработки персональных данных

1. Общие положения

1.1 Настоящая Политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с частью 2 пункта 1 статьи 18.1 Федерального закона РФ «Оперсональных данных» №152-ФЗ от 27 июля 2006 года и действует в отношении всех персональных данных (далее – ПДн), которые Государственное бюджетное учреждение здравоохранения Республики Башкортостан Бакалинская центральная районная больница (далее – Учреждение) может получить от субъекта персональных данных в определенных целях в качестве оператора персональных данных.

1.2 Под субъектами персональных данных в настоящей Политике понимаются:

1.2.1. Сотрудники Учреждения, состоящие в трудовых, гражданско-правовых отношениях с Учреждением.

1.2.2. Пациенты (и/или их законные представители), обратившиеся в Учреждение с целью получения медицинской помощи.

1.2.3. Лица, состоящие в гражданско-правовых отношениях с другими юридическими лицами, направленные на прохождение медосмотра.

1.2.4. Положения настоящего документа распространяются на весь объем ПДн, обрабатываемых в Управляющей, полученных как до, так и после утверждения настоящей Политики.

2. Цели сбора и обработки ПДН

2.1 Учреждение собирает и хранит ПДн сотрудника, в целях заключения трудового договора и исполнения его условий, осуществления прав и обязанностей работодателя в соответствии с трудовым законодательством РФ, ведения бухгалтерского учета и отчетности, кадрового учета, продвижения Работника по службе.

2.2 Учреждение собирает и хранит ПДн пациентов (и/или их законных представителей) в целях исполнения действующего законодательства Российской Федерации в области охраны здоровья граждан, улучшению качества жизни граждан, оказания медицинской помощи, исполнения программы обязательного медицинского страхования и ведения медицинской статистики[1].

2.3 Учреждение собирает и хранит ПДн лиц, направленных на прохождение медосмотра, в целях исполнения порядка осуществления процедуры медосмотра, определенной законодательством РФ[2].

---

[1] ФЗ «Об основах здоровья граждан в Российской Федерации»
[2] Трудовой кодекс, СанПиН

3. Условия обработки ПДН и их передачи третьим лицам

3.1 Обработка ПДн осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи, обезличивания, блокирования, удаления, уничтожения ПДн.

3.2 Обработка осуществляется как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка), с передачей по внутренней сети Учреждения и с передачей по сети Интернет (с использованием средств криптографической защиты информации).

3.3 Срок хранения для ПДн в электронном виде ограничивается сроком исковой давности, архивного хранения и определен в Перечне обрабатываемых ПДн.

3.4 Срок хранения ПДн без использования средств автоматизации определяется номенклатурой дел.

3.4.1. Для документов по личному составу (сотрудники) составляет 75 лет.

3.4.2. Для амбулаторной карты пациента - 5 лет со дня последнего визита. Амбулаторная карта перемещается в архив Учреждения. По истечению 25 лет хранения по решению комиссии амбулаторная карта уничтожается или продлевается срок хранения (на основании экспертизы ценности).

3.4.3. Амбулаторная карта пациента подлежит хранению только в регистратуре учреждения.

3.5 По истечению указанных сроков ПДн в электронном виде удаляются или обезличиваются; обрабатываемые без использования средств автоматизации уничтожаются или передаются на архивное хранение.

3.6 Учреждение вправе передавать ПДн субъектов третьим лицам в случаях, предусмотренных законодательством Российской Федерации, а также при наличии письменного согласия субъекта на передачу его ПДн.

3.7 При обработке ПДн субъектов Учреждение руководствуется Трудовым кодексом Российской Федерации, Федеральным законом РФ «О персональных данных» №152-ФЗ от 27 июля 2006 года и другими нормативно-правовыми актами в области защиты ПДн.

3.8 Законченные делопроизводством документы и дела, содержащиеся ПДн субъектов, хранятся в архиве Учреждения в соответствии с установленными сроками и условиями хранения.

4. Изменение данных

4.1 Субъекты ПДн могут внести, дополнить или изменить свои ПДн.

4.2 Субъекты ПДн могут потребовать прекращения обработки и/или удаления своих ПДн.

5. Меры, применяемые для защиты данных

5.1 Учреждение гарантирует конфиденциальность ПДн и предоставляет доступ к ним только уполномоченным Работникам, подписавшим обязательство о неразглашении информации, содержащей ПДн.

5.2 Все сотрудники Учреждения, имеющие доступ к персональным данным, соблюдают правила и исполняют требования Положения об обработке ПДн.

5.3 Учреждение принимает необходимые и достаточные организационные и технические меры для защиты ПДн от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.4 Все рабочие места, на которых обрабатываются ПДн реализуют механизмы разграничения прав доступа, антивирусной защиты, парольной защиты.

6. Права субъектов ПДН

6.1 Субъект ПДн имеет право запрашивать у Учреждения следующие сведения:

- подтверждение факта обработки ПДн;
- правовые основания и цели обработки ПДн;
- цели и применяемые способы обработки ПДн;
- наименование и место нахождения, сведения о лицах (за исключением сотрудников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании ФЗ;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ;
- сроки обработки ФЗ, в том числе сроки их хранения;
- порядок осуществления субъектом прав, предусмотренных законодательством;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные законодательством

6.2 Субъект ПДн имеет право требовать от Учреждения уточнения своих ПДн, их блокирования или уничтожения.

6.3 Субъект ПДн не должен отказываться от своих прав на сохранение личной и семейной тайны.

6.4 Если субъект ПДн считает, что Учреждение осуществляет обработку его ПДн с нарушением требований действующего законодательства РФ или иным образом нарушает его права и свободы, субъект вправе обжаловать действия или бездействие Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

7. Изменение политики, применимое законодательство

7.1 Учреждение имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее утверждения Главным врачом, если иное не предусмотрено новой редакцией Политики.

7.2 Действующая редакция хранится в месте нахождения Учреждения по адресу: 452650, Республика Башкортостан, Бакалинский р-н, с. Бакалы, ул. Шакирьянова, 2

7.3 К настоящей Политике и отношениям между Субъектами ПДн и Учреждением подлежит применению право Российской Федерации

Приложение № 3
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

Перечень персональных данных, обрабатываемых в ГБУЗ РБ Бакалинская ЦРБ в связи с реализацией трудовых отношений;

1. паспорт
2. трудовая книжка
3.сертификат
4. диплом
5. СНИЛС
6. ИНН
7. удостоверение о повышении квалификации
8. удостоверения, свидетельство о дополнительном образовании
9. удостоверение о присвоении квалификационной категории
10. свидетельство о браке
11. свидетельство о рождение ребенка
12. военный билет
13. удостоверение об окончании интернатуры
14. диплом об ординатуре
15.свидетельство об аккредитации

Приложение № 4
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

Перечень должностей ГБУЗ РБ Бакалинская ЦРБ ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных

1. программист
2. регистратор
3. медицинский статистик
4. врач - статист
5. начальник отдела кадров
6. специалист отдела кадров
7. мед. сестра по приему вызовов отделения скорой помощи
8. врачи и средние медицинские работники поликлиники
9. врачи и средние медицинские работники детской консультации
10. врачи и средние медицинские работники женской консультации
11. архивариус
12. врачи и средние медицинские работники стационара
13. фельдшера
14. медицинская сестра
15. оператор
16. медицинская сестра приемного отделения
17. специалист по ОТ
18. специалист по ГО
19. юрист
20. секретарь
21. делопроизводитель

Приложение № 5
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

Перечень персональных данных, обрабатываемых в ГБУЗ РБ Бакалинская ЦРБ в связи с осуществлением медицинской деятельности

1. Паспортные данные
2. Свидетельство о рождении
3. СНИЛС
4. ИНН
5. Страховой полис
6. Место работы, должность, профессия
7. Удостоверение об инвалидности
8. Контактный номер телефона

Приложение № 6
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

Перечень информационных систем персональных данных

№ п/п	Наименование информационной системы персональных данных	Оператор информационной системы	Месторасположение информационной системы
1	РМИАС	ООО ЭМСИС	РБ, г. Уфа
2	1С: Бухгалтерия	ГБУЗ РБ Бакалинская ЦРБ	РБ, с. Бакалы
3	СЭД Дело	ЦИКТ РБ	РБ, г.Уфа
4	ЕГИСЗ	Росминздрав	РФ, г. Москва

Приложение № 7
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

ПЕРЕЧЕНЬ
мест хранения персональных данных (ПДн), обрабатываемых в ГБУЗ РБ Бакалинская ЦРБ

№ п/п	Подразделение	Место нахождения	Наименование документа, содержащего ПДн
1	Отдел кадров	шкаф/сейф	Личные дела сотрудников, трудовые книжки, приказы
2	Бухгалтерия	Архив	Индивидуальные сведения о трудовом стаже, заработке (вознаграждении), доходе и начисленных страховых взносах застрахованного лица; Расчетные (расчетно-платежные) ведомости; Листки нетрудоспособности
3	Архивариус	Архив	ГАП, КВС, Выписки
4	Регистратура	Картотека	Амбулаторные карты пациентов

Приложение № 8
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

МОДЕЛЬ
угроз безопасности персональных данных при их обработке в информационной системе персональных данных

1. Общие положения

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных (далее — ИСПДн) в ГБУЗ РБ Бакалинская ЦРБ (далее — Модель угроз, ЦРБ соответственно) разработана в соответствии со следующими действующими нормативно-методическими документами по защите персональных данных:

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная Федеральной службой по техническому и экспортному контролю14 февраля 2008 года(далее - Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных);
- Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных, утвержденная Федеральной службой по техническому и экспортному контролю15 февраля 2008года);
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные Федеральной службой безопасности Российской Федерации 21 февраля 2008года

№ 149/6/6-622;

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные Федеральной службой безопасности Российской Федерации 21 февраля 2008года

№ 149/54-144;

- Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные приобработке

персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные Федеральной службой безопасности Российской Федерации 31 марта 2015 года № 149/7/2/6-432.

Настоящая Модель угроз содержит систематизированный перечень угроз безопасности персональных данных при их обработке в ИСПДн. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности персональных данных, которые ведут к ущербу жизненно-важных интересов личности, общества и государства.

Модель угроз содержит данные по угрозам безопасности персональных данных, обрабатываемых в ИСПДн, связанным:

- с перехватом (съемом) персональных данных (далее – ПДн) по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в нихПДн;
- с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц ЦРБ как оператора персональных данных (далее - оператор), администраторов ИСПДн, разработчиков ИСПДн и их подсистем.

Модель угроз разработана для ИСПДн с учетом ее назначения, условий и особенностей функционирования.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
-разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности ИСПДн;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроль обеспечения уровня защищенности персональных данных.

В Модели угроз дано обобщенное описание ИСПДн как объекта защиты, возможных источников угроз безопасности персональных данных (далее - УБПДн), основных классов уязвимостей ИСПДн, возможных видов

неправомерных действий и деструктивных воздействий на ПДн, а также основных способов их реализации.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Модель угроз может быть пересмотрена по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений ИСПДн, а также по результатам мероприятий по контролю выполнения требований к обеспечению безопасности ПДн при их обработке в информационной системе.

2. Возможные последствия нарушения безопасности персональных данных

Возможными последствиями нарушения безопасности персональных данных, обрабатываемых в ИСПДн, являются:

- разглашение персональных данных, несанкционированное изменение ПДн субъектов персональных данных и причинение им физического, материального, финансового или морального ущерба;
- причинение материального ущерба оператору;
- вред репутации оператора в обществе.

Разглашение персональных данных субъектов персональных данных и причинение им физического, материального, финансового или морального ущерба может проявляться в виде:

- незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;
- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием персональных данных;
- нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

Раздел III. Объекты угроз

Объектами угроз в ИСПДн, подлежащими защите, являются информационные ресурсы, содержащие персональные данные, информационные технологии, технические и программные средства, используемые для обработки персональных данных, программные средства защиты.

Глава 1. Основные ресурсы, содержащие персональные данные

Основными информационными ресурсами, содержащими персональные данные, в ИСПДн, являются ресурсы:

- «РМИАС»;
- «1С — Бухгалтерия для бюджетных организаций»;
- Сахарный диабет;
- ГосУслуги
- автоматизированный расчет зарплаты и подготовка отчетности АМБА;
- электронные документы и

таблицы, содержащие персональные данные сотрудников оператора.

Глава 2. Информация, формируемая в процессе создания и обработки персональных данных, но не содержащая персональных данных

В процессе обработки персональных данных в ИСПДн осуществляется формирование информации, не являющейся персональными данными, но получение которой злоумышленником способствует получению им доступа к персональным данным. По этой причине к объектам угроз относится:

- ключевая, аутентифицирующая и парольнаяинформация;
- криптографически опаснаяинформация;
- конфигурационная и управляющаяинформация;
- информация в электронных журналахрегистрации;
- остаточная информация на носителяхинформации;
- информация, подверженная съему по побочному электромагнитному излучению инаводкам.

Раздел IV. Характеристики безопасности персональных данных

Для ПДн и объектов, которые могут выступать в качестве объектов угроз и требуют защиты, необходимо обеспечить выполнение следующих характеристик безопасности:

- конфиденциальность;
- целостность;
- доступность.

Обеспечение других характеристик безопасности в ИСПДн не требуется, так как их нарушение не может привести к негативным последствиям для субъектов Пдн.

Раздел V. Модель нарушителя безопасности персональных данных

Глава 3. Описание нарушителей

В качестве нарушителя безопасности персональных данных могут выступать физические лица или организации, которые преднамеренно или случайно совершают действия, в результате которых нарушаются заданные характеристики безопасности персональных данных.

В зависимости от прав доступа к ресурсам ИСПДн, нарушители подразделяются на два типа:

- внешние;
- внутренние.

Внешними нарушителями могут являться:

- организованные преступные группы, сообщества;
- бывшие сотрудники оператора;
- недобросовестные партнеры.

Внутренними (потенциальными) нарушителями являются сотрудники оператора, находящиеся в пределах контролируемой зоны.

Привилегированные пользователи ИСПДн (администраторы), которые осуществляют техническое управление и обслуживание аппаратных и программных средств ИСПДн, в том числе и средств защиты, включая их настройку, конфигурирование и распределение ключевой и парольной документации, относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

Предполагается, что потенциальные нарушители:

- не могут организовывать или заказывать работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды их функционирования;
- являются, в силу специфики информации ИСПДн, одиночками, самостоятельно осуществляющими освоение способов, подготовку и проведение атак.

Основными объектами атак являются:

- документация, технические и программные компоненты;
- ресурсы персональных данных;
- ключевая, аутентифицирующая и парольная информация;
- криптографически опасная информация;
- аппаратные и программные средства защиты;
- технические и программные компоненты среды функционирования криптосредств;
- помещения, в которых размещены ресурсыИСПДн.

Целью атаки является неправомерный доступ к информации или к вычислительным ресурсам ИСПДн как с умыслом нанесения ущерба оператору, так и без такого умысла.

Глава 4. Предположения об имеющейся у нарушителя информации об объектах атак

Предполагается, что потенциальный нарушитель не располагает исходными текстами прикладного программного обеспечения.

Разработчики прикладного программного обеспечения относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

Глава 5. Описание каналов атак

Основными каналами атак являются:

- визуальный канал, который может позволить получить персональные данные путем просматривания документированной и отображаемой на технических средствах информации;
- физический доступ к документации и в помещения, в которых расположены ресурсы ИСПДн;
- каналы связи, не защищенные от несанкционированного доступа к информации организационно-техническими мерами;
- средства обработки информации;
- машинные носители информации.

Раздел VI. Основные угрозы безопасности персональных данных

Формирование Модели угроз осуществлено на основе определенных ранее угроз безопасности персональных данных при их обработке. Проведен

анализ перечня угроз безопасности персональных данных с учетом оперативной обстановки, складывающейся вокруг оператора, имеющихся доступных материалов о реально зафиксированных угрозах безопасности персональных данных с учетом опыта оператора, а также имеющихся на общедоступном рынке средств защиты и средств технической разведки в информационной сфере.

При этом были выполнены требования нормативных правовых актов и учтены положения методических документов Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

Перечень и актуальность угроз безопасности персональных данных сформирован исходя из анализа непреднамеренных (ошибочных, случайных) действий персонала оператора, учета условий жизнеобеспечения и системы энергоснабжения ИСПДн, а также влияния иных техногенных и природных факторов (стихийные бедствия ит.п.).

Глава 6. Оценка уровня исходной защищенности информационной системы персональных данных

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению			
локальная ИСПДн, развернутая в пределах одного здания	-	+	-
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая одноточечный выход в сеть общего пользования	-	+	-
3. По встроенным (легальным) операциям с записями баз ПДн:			
чтение, поиск, запись, удаление, сортировка, модификация, передача	-	-	+
4. По разграничению доступа к ПДн:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъектПДн	-	+	-
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	-	-
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е.присутствует	-	-	+

информация, позволяющая идентифицировать субъекта ПДн)			
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая часть ПДн	-	+	-
Характеристики ИСПДн, %	14	57	29
Исходный уровень защищенности		5	

Поскольку более 70% показателей исходной защищенности ИСПД имеют значение не ниже «средний уровень исходной защищенности», то согласно раздела 2 «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ИСПДн относится к информационным системам со средней степенью исходной защищенности и соответствующий числовой коэффициент (Yi) равен 5.

Глава 7. Определение вероятности реализации угроз безопасности персональных данных

Вероятность реализации угроз безопасности ПДн определена экспертным методом в соответствии с Методикой и на основании результатов обследования ИСПДн.

§ 1. Угрозы утечки по техническим каналам

Утечка акустической информации

Речевое воспроизведение защищаемой информации в ИСПДн непроизводится.

Вероятность реализации угрозы – маловероятно.

Утечка видовой информации

Со средств отображения индивидуального пользования.

Мониторы рабочих станций пользователей расположены таким образом, что исключен несанкционированный просмотр отображаемой на них информации посторонними лицами. Окна помещений оборудованы жалюзи. Вероятность реализации угрозы – маловероятно.

С печатных документов.

Принтеры рабочих станций расположены таким образом, что исключен несанкционированный просмотр информации, выводимой на печать, документы, содержащие защищаемую информацию, хранятся на рабочих столах. Окна помещений оборудованы жалюзи. Вероятность реализации угрозы – маловероятно.

Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств

В ИСПДн используются технические средства, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по

безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники. Вероятность реализации угрозы – маловероятно.

Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны

В ИСПДн используются технические средства, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности иэргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники. Вероятность реализации угрозы – маловероятно.

Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации

Меры по защите информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны, не удовлетворяют требованиям нормативных документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации. Несанкционированный доступ посторонних лиц к техническим средствам, входящим в состав ИСПДн, исключен. Вероятность реализации угрозы – средняя.

§ 2. Несанкционированный доступ к информации

Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн

Кража ПЭВМ.

Охрана здания осуществляется, на входе в здание расположен пост охраны. Помещения оборудованы охранно-пожарной сигнализацией. Вероятность реализации угрозы – маловероятно.

Кража носителей информации.

В ИСПДн используются съемные носители информации. Учет съемных носителей информации не ведется. Вероятность реализации угрозы –средняя.

Кража ключей и атрибутов доступа.

Аппаратные идентификаторы и ключи доступа не используются. Вероятность реализации угрозы – маловероятно.

Нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн.

Все коммутационное оборудование ИСПДн находится в серверном помещении, доступ в которое ограничен. Линии связи внутри здания проложены в кабель-каналах, а также под фальш-потолками. Вероятность реализации угрозы –маловероятно.

Внедрение аппаратных закладок в технические средства ИСПДн.

Системные блоки технических средств, входящих в состав ИСПДн, не опечатаны, что делает возможным незамеченное внедрение аппаратных закладок в данные технические средства. Вероятность реализации угрозы – средняя.

Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн.

Обслуживание технических средств производится без присутствия администратора безопасности. Вероятность реализации угрозы – средняя.

Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно- аппаратных и программных средств (в том числе программно-математических воздействий)

Воздействие вредоносных программ.

На серверах и автоматизированных рабочих местах (далее — АРМ) пользователей установлено средство антивирусной защиты

Производится регулярное обновление антивирусных баз. Вероятность реализации угрозы – маловероятно.

Недекларированные возможности общесистемного и прикладного программного обеспечения.

В ИСПДн используется нелицензионное программное обеспечение. В ИСПДн отсутствуют средства модификации объектного кода программного обеспечения. Вероятность реализации угрозы – средняя.

Ошибки в общесистемном и прикладном программном обеспечении.

В ИСПДн используется нелицензионное программное обеспечение. Средства модификации объектного кода программного обеспечения отсутствуют. Ведется резервное копирование баз данных защищаемой информации. Вероятность реализации угрозы – средняя.

Установка программного обеспечения, не связанного с исполнением служебных обязанностей.

У пользователей ИСПДн имеются учетные записи без прав администрирования, что исключает возможность установки пользователями программного обеспечения, не связанного с выполнением должностных обязанностей, в том числе для поиска уязвимостей в ИСПДн и анализа информации, циркулирующей в ИСПДн. Вероятность реализации угрозы – маловероятно.

Неумышленные деструктивные действия персонала

Утрата ключей и атрибутов доступа.

Аппаратные идентификаторы и ключи доступа не используются. Вероятность реализации угрозы – маловероятно.

Непреднамеренная модификация (уничтожение) информации сотрудниками.

У пользователей ИСПДн имеются учетные записи без прав администрирования.

Вероятность реализации угрозы – аловероятно.

Непреднамеренное отключение средств защиты.

У пользователей ИСПДн имеются учетные записи без прав администрирования.

Вероятность реализации угрозы – аловероятно.

Вывод из строя аппаратно-программных средств вследствие ошибочных действий.

Отсутствуют инструкции пользователей по работе с защищаемой информацией и техническими средствами. Вероятность реализации угрозы – средняя.

Умышленные деструктивные действия персонала

Копирование баз данных администратором.

У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Вероятность реализации угрозы – маловероятно.

Накопление данных пользователем информационной системы.

У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Вероятность реализации угрозы – маловероятно.

Злонамеренное разрушение (искажение) информации.

У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Ведется резервное копирование баз данных защищаемой информации администратором. Вероятность реализации угрозы – маловероятная.

Злонамеренное блокирование данных.

У пользователей ИСПДн имеются учетные записи без прав администрирования. Ведется резервное копирование баз данных защищаемой информации. Вероятность реализации угрозы – низкая.

Фальсификация данных.

У пользователей ИСПДн имеются учетные записи без прав администрирования. Аудит действий пользователей не ведется. Ведется резервное копирование баз данных защищаемой информации. Вероятность реализации угрозы – маловероятно.

Несанкционированный доступ персонала информационной системы к ресурсам. У пользователей ИСПДн имеются учетные записи без прав администрирования.

Аудит действий пользователей не ведется. Матрица доступа пользователей к защищаемым информационным ресурсам формализована. Вероятность реализации угрозы – маловероятно.

Компрометация аутентификатора.

Правила хранения парольной информации отсутствуют. Вероятность реализации угрозы – высокая.

Компрометация ключа средства криптографической защиты информации (далее

- СКЗИ.

Ответственный пользователь криптосредств не назначен. Журнал учета криптографических ключей не ведется. Вероятность реализации угрозы – средняя.

Нарушение функционирования средства защиты.

У пользователей ИСПДн имеются учетные записи без прав администрирования.

Вероятность реализации угрозы – маловероятно.

Произвольное создание точек входа в систему за счет неправомерных действий.

Все коммутационное оборудование ИСПДн находится в серверном помещении, доступ в которое ограничен. Линии связи внутри здания проложены в кабель-каналах, а также под фальш-потолками. Вероятность реализации угрозы –маловероятно.

Угрозы несанкционированного доступа по каналам связи

Перехват передаваемой информации за пределами контролируемой зоны.

В ИСПДн производится передача защищаемой информации через линии связи, выходящие за границы контролируемой зоны. Меры по защите информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны, не удовлетворяют требованиям нормативных документов Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации. Вероятность реализации угрозы – высокая.

Перехват в пределах контролируемой зоны внешними нарушителями.

Внутри здания ЦРБ исключено неконтролируемое пребывание посторонних лиц. Вероятность реализации угрозы – маловероятно.

Перехват в пределах контролируемой зоны внутренними нарушителями.

У пользователей ИСПДн имеются учетные записи без прав администрирования, не дающие возможность установки программ-сниферов. Вероятность реализации угрозы – маловероятно.

Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи с административными правами. Вероятность реализации угрозы – средняя.

Угрозы выявления паролей по сети.

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн не имеется учетных записей с административными правами, не предоставляющими возможность установки программ-сниферов. Вероятность реализации угрозы – маловероятно.

Угрозы навязывания ложного маршрута сети.

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн отсутствуют учетные записи с административными правами. Вероятность реализации угрозы – маловероятно.

Угрозы подмены доверенного объекта в сети.

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи

безправадминистрирования. Вероятность реализации угрозы – маловероятно.

Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

Угрозы типа «Отказ в обслуживании».

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

Угрозы удаленного запуска приложений.

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, в наличии. У пользователей ИСПДн имеются учетные записи без прав администрирования. Вероятность реализации угрозы – маловероятно.

Вторжение в ИСПДн по информационно-телекоммуникационным сетям.

ИСПДн имеет подключение к сетям связи общего пользования. Средства межсетевого экранирования, удовлетворяющие требованиям нормативных документов Федеральной службы по техническому и экспортному контролю, отсутствуют. Вероятность реализации угрозы – средняя.

Искажение в каналах передачи.

Передача данных производится по оптико-волоконным линиям связи, при передаче используется избыточное кодирование информации. Вероятность реализации угрозы –маловероятно.

§ 3. Угрозы стихийного характера

Нарушение электроснабжения

Внешнего.

Серверное и коммутационное оборудование ИСПДн подключено к системе источников бесперебойного питания. Вероятность реализации угрозы – маловероятно.

Объектового.

Серверное и коммутационное оборудование ИСПДн подключено к системе источников бесперебойного питания. Вероятность реализации угрозы – маловероятно.

Стихийное бедствие, катастрофа

В связи с географическим расположением оператора, отсутствуют объективные предпосылки для осуществления угрозы. Вероятность реализации угрозы – маловероятно.

№ п/п	Угроза	Вероятность реализацииугрозы (Y2)	Коэффициент реализуемости угрозы Y. Возможность реализации угрозы	
1	Утечки по техническим каналам			
1.1	Утечка акустической информации	маловероятно (0)	низкая	0,25
1.2	Утечка видовой информации:			
1.2.1	со средств отображения индивидуального пользования	маловероятно (0)	низкая	0,25
1.2.2	со средств коллективного отображения	маловероятно (0)	низкая	0,25
1.2.3	с печатных документов	маловероятно (0)	низкая	0,25
1.3	Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств	маловероятно (0)	низкая	0,25
1.4	Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	маловероятно (0)	низкая	0,25
1.5	Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	средняя (5)	средняя	0,5
2	Несанкционированный доступ к информации			
2.1	Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн:			

2.1.1	кража персональных электронно-вычислительных машин (далее - ПЭВМ)	маловероятно (0)	низкая	0,25
2.1.2	кража носителей информации	средняя (5)	средняя	0,5
2.1.3	кража ключей и атрибутов доступа	маловероятно (0)	низкая	0,25
2.1.4	нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн	маловероятно (0)	низкая	0,25
2.1.5	внедрение аппаратных закладок в технические средства ИСПДн	средняя (5)	средняя	0,5
2.1.6	несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн	маловероятно (0)	низкая	0,25
2.2	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):			
2.2.1	воздействие вредоносных программ	маловероятно (0)	низкая	0,25
2.2.2	недекларированные возможности общесистемного и прикладного програмного обеспечения (далее - ПО)	маловероятно (0)	низкая	0,25
2.2.3	ошибки в общесистемном и прикладном ПО	маловероятно (0)	низкая	0,25
2.2.4	установка ПО не связанного с исполнением служебных обязанностей	маловероятно (0)	высокая	0,25
2.3	Неумышленные деструктивные действия персонала:			
2.3.1	утрата ключей и атрибутов доступа	маловероятно (0)	низкая	0,25
2.3.2	непреднамеренная модификация (уничтожение) информации сотрудниками	средняя (5)	средняя	0,5

2.3.3	непреднамеренное отключение средств защиты	высокая (10)	высо кая	0,7 5
2.3.4	вывод из строя аппаратно-программных средств вследствие ошибочных действий	средняя (5)	средн яя	0,5
2.4	Умышленные деструктивные действия персонала:			
2.4.1	произвольное копирование баз данных	средняя (5)	средн яя	0,5
2.4.2	накопление данных пользователем информационной системы	средняя (5)	средн яя	0,5
2.4.3	злонамеренное разрушение (искажение) информации	средняя (5)	средн яя	0,5
2.4.4	злонамеренное блокирование данных	низкая (2)	средн яя	0,3 5
2.4.5	фальсификация данных	низкая (2)	средн яя	0,3 5
2.4.6	несанкционированный доступ персонала информационной системы к ресурсам	средняя (5)	средн яя	0,5
2.4.7	компрометация аутентификатора	высокая (10)	высо кая	0,7 5
2.4.8	компрометация ключа СКЗИ	средняя (5)	средн яя	0,5
2.4.9	нарушение функционирования средства защиты	высокая (10)	низка я	
2.4.10	произвольное создание точек входа в систему за счет неправомерных действий	маловероятно (0)	низка я	0,2 5
2.5	Угрозы несанкционированного доступа по каналам связи:			
2.5.1	перехват передаваемой информации за переделами контролируемой зоны	маловероятно (0)	низка я	0,2 5
2.5.2	перехват в пределах контролируемой зоны внешними нарушителями	маловероятно (0)	низка я	0,2 5
2.5.3	перехват в пределах контролируемой зоны внутренними нарушителями	средняя (5)	средн яя	0,5

2.5.4	угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая (2)	средняя	0,35
2.5.5	угрозы выявления паролей по сети	низкая (2)	средняя	0,35
2.5.6	угрозы навязывание ложного маршрута сети	низкая (2)	средняя	0,35
2.5.7	угрозы подмены доверенного объекта в сети	средняя (5)	средняя	0,5
2.5.8	угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя (5)	средняя	0,5
2.5.9	угрозы типа «Отказ в обслуживании»	средняя (5)	средняя	0,5
2.5.10	угрозы удаленного запуска приложений	средняя (5)	средняя	0,5
2.5.11	угрозы внедрения по сети вредоносных программ	маловероятно (0)	низкая	0,25
2.5.12	вторжение в ИСПДн по информационно-телекоммуникационным сетям	средняя (5)	средняя	0,5
2.5.13	искажение в каналах передачи	маловероятно (0)	низкая	0,25
3	Угрозы стихийного характера			
3.1	Нарушение электроснабжения:			
3.1.1	внешнего	маловероятно (0)	низкая	0,25
3.1.2	объектового	маловероятно (0)	низкая	0,25
3.2	Стихийное бедствие, катастрофа	маловероятно (0)	низкая	0,25

§ 4. Определение опасности угроз безопасности персональных данных

Определение опасности угроз безопасности ПДн проведено экспертным методом на основе опроса экспертов (специалистов в области защиты информации) с учетом результатов обследования ИСПДн. Результаты определения опасности угроз с мнениями экспертов приведены ниже:

№ п/п	Угроза	Показатель опасности

		угрозы
1	Утечки по техническим каналам	
1.1	Утечка акустической информации	средняя
1.2	Утечка видовой информации:	
1.2.1	со средств отображения индивидуального пользования	средняя
1.2.2	со средств коллективного отображения	средняя
1.2.3	с печатных документов	средняя
1.3	Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств	средняя
1.4	Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	средняя
1.5	Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	средняя
2	Несанкционированный доступ к информации	
2.1	Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн:	
2.1.1	кража ПЭВМ	средняя
2.1.2	кража носителей информации	высокая
2.1.3	кража ключей и атрибутов доступа	средняя
2.1.4	нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн	низкая
2.1.5	внедрение аппаратных закладок в технические средства ИСПДн	средняя

2.1.6	несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн	средняя
2.2	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):	
2.2.1	воздействие вредоносных программ	средняя
2.2.2	недекларированные возможности общесистемного и прикладного ПО	средняя
2.2.3	ошибки в общесистемном и прикладном ПО	средняя
2.2.4	установка ПО не связанного с исполнением служебных обязанностей	средняя
2.3	Неумышленные деструктивные действия персонала:	
2.3.1	утрата ключей и атрибутов доступа	средняя
2.3.2	непреднамеренная модификация (уничтожение) информации сотрудниками	средняя
2.3.3	непреднамеренное отключение средств защиты	средняя
2.3.4	вывод из строя аппаратно-программных средств вследствие ошибочных действий	средняя
2.4	Умышленные деструктивные действия персонала:	
2.4.1	произвольное копирование баз данных	низкая
2.4.2	накопление данных пользователем информационной системы	высокая
2.4.3	злонамеренное разрушение (искажение) информации	средняя
2.4.4	злонамеренное блокирование данных	низкая
2.4.5	фальсификация данных	средняя
2.4.6	несанкционированный доступ персонала информационной системы к ресурсам	средняя
2.4.7	компрометация аутентификатора	средняя

2.4.8	компрометация ключа СКЗИ	высо кая
2.4.9	нарушение функционирования средства защиты	сред няя
2.4.10	произвольное создание точек входа в систему за счет неправомерных действий	средн яя
2.5	Угрозы несанкционированного доступа по каналам связи:	
2.5.1	перехват передаваемой информации за переделами контролируемой зоны	низка я
2.5.2	перехват в пределах контролируемой зоны внешними нарушителями	средн яя
2.5.3	перехват в пределах контролируемой зоны внутренними нарушителями	высо кая
2.5.4	угрозы сканирования, направленные на выявление типа или типов используемых операционных систем,сетевых адресов рабочих станций ИСПДн, топологиисети, открытых портов и служб, открытых соединений и др.	средн яя
2.5.5	угрозы выявления паролей по сети	средн яя
2.5.6	угрозы навязывание ложного маршрута сети	средн яя
2.5.7	угрозы подмены доверенного объекта в сети	средн яя
2.5.8	угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средн яя
2.5.9	угрозы типа «Отказ в обслуживании»	средн яя
2.5.10	угрозы удаленного запуска приложений	средн яя
2.5.11	угрозы внедрения по сети вредоносных программ	средн яя
2.5.12	вторжение в ИСПДн по информационно-телекоммуникационным сетям	высо кая
2.5.13	искажение в каналах передачи	средн яя
3	Угрозы стихийного характера	
3.1	Нарушение электроснабжения:	
3.1.1	внешнего	средн яя
3.1.2	объектового	средн яя

3.2	Стихийное бедствие, катастрофа	средняя

§ 5. Определение актуальности угроз безопасности персональных данных

Актуальность угрозы в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных определяется с учетом оценок вероятности ее реализации и опасности. Результаты приведены ниже.

№ п/п	Форма реализации угрозы	Интерпретация реализуемости угрозы	Опасность угрозы	Актуальность угрозы
1	Утечки по техническим каналам			
1.1	Утечка акустической информации	низкая	средняя	неактуальная
1.2	Утечка видовой информации:			
1.2.1	со средств отображения индивидуального пользования	низкая	средняя	неактуальная
1.2.2	со средств коллективного отображения	низкая	средняя	неактуальная
1.2.3	с печатных документов	низкая	средняя	неактуальная
1.3	Утечка информации за счет побочных электромагнитных излучений информативных сигналов от технических средств	низкая	средняя	неактуальная
1.4	Утечка информации за счет наводок информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны	низкая	средняя	неактуальная

1.5	Утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	средняя	средняя	актуальная
2	Несанкционированный доступ к информации			
2.1	Угрозы уничтожения, хищения, модификации технических средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн:			
2.1.1	кража ПЭВМ	низкая	средняя	неактуальная
2.1.2	кража носителей информации	средняя	высокая	актуальная
2.1.3	кража ключей и атрибутов доступа	низкая	средняя	неактуальная
2.1.4	нарушение функционирования телекоммуникационных каналов, технических средств ИСПДн	низкая	низкая	неактуальная
2.1.5	внедрение аппаратных закладок в технические средства ИСПДн	средняя	средняя	актуальная
2.1.6	несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) технических средств ИСПДн	низкая	средняя	неактуальная
2.2	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):			
2.2.	воздействие	низкая	средн	неактуаль

1	вредоносных программ		яя	ная
2.2.2	недекларированные возможности общесистемного и прикладного ПО	низкая	средняя	неактуальная
2.2.3	ошибки в общесистемном и прикладном ПО	низкая	средняя	неактуальная
2.2.4	установка ПО не связанного с исполнением служебных обязанностей	средняя	высокая	актуальная
2.3	Неумышленные деструктивные действия персонала:			
2.3.1	утрата ключей и атрибутов доступа	низкая	средняя	неактуальная
2.3.2	непреднамеренная модификация (уничтожение) информации сотрудниками	средняя	средняя	актуальная
2.3.3	непреднамеренное отключение средств защиты	средняя	средняя	актуальная
2.3.4	вывод из строя аппаратно-программных средств вследствие ошибочных действий	средняя	средняя	актуальная
2.4	Умышленные деструктивные действия персонала:			
2.4.1	произвольное копирование баз данных	низкая	высокая	актуальная
2.4.2	накопление данных пользователем информационной системы	средняя	высокая	актуальная
2.4.3	злонамеренное разрушение (искажение) информации	средняя	высокая	актуальная
2.4.4	злонамеренное блокирование	низкая	средняя	актуальная

	данных			
2.4.5	фальсификация данных	средняя	высокая	актуальная
2.4.6	несанкционированный доступ персонала информационной системы (далее - ИС) к ресурсам	средняя	средняя	актуальная
2.4.7	компрометация аутентификатора	высокая	средняя	актуальная
2.4.8	компрометация ключа СКЗИ	средняя	высокая	актуальная
2.4.9	нарушение функционирования средства защиты	низкая	высокая	актуальная
2.4.10	произвольное создание точек входа в систему за счет неправомерных действий	низкая	средняя	неактуальная
2.5	Угрозы несанкционированного доступа по каналам связи:			
2.5.1	перехват передаваемой информации за пределами контролируемой зоны	низкая	низкая	неактуальная
2.5.2	перехват в пределах контролируемой зоны внешними нарушителями	низкая	средняя	неактуальная
2.5.3	перехват в пределах контролируемой зоны внутренними нарушителями	средняя	высокая	актуальная
2.5.4	угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений	средняя	средняя	актуальная

	и др.			
2.5.5	угрозы выявления паролей по сети	средняя	средняя	актуальная
2.5.6	угрозы навязывание ложного маршрута сети	средняя	средняя	актуальная
2.5.7	угрозы подмены доверенного объекта в сети	средняя	средняя	актуальная
2.5.8	угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя	средняя	актуальная
2.5.9	угрозы типа «Отказ в обслуживании»	средняя	средняя	актуальная
2.5.10	угрозы удаленного запуска приложений	средняя	средняя	актуальная
2.5.11	угрозы внедрения по сети вредоносных программ	низкая	средняя	неактуальная
2.5.12	вторжение в ИСПД по информационно-телекоммуникационным сетям	средняя	высокая	актуальная
2.5.13	искажение в каналах передачи	низкая	средняя	неактуальная
3	Угрозы стихийного характера			
3.1	Нарушение электроснабжения:			
3.1.1	внешнего	низкая	средняя	неактуальная
3.1.2	объектового	низкая	средняя	неактуальная
3.2	Стихийное бедствие, катастрофа	низкая	средняя	неактуальная

Раздел VII. Заключение

Таким образом, в отношении персональных данных, обрабатываемых в ИСПДн, актуальными являются следующие угрозы безопасности:

- утечка информации за счет радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработкиинформации;
- кража носителейинформации;
- внедрение аппаратных закладок в технические средстваИСПДн;
-непреднамеренная модификация (уничтожение) информации сотрудниками;
-непреднамеренное отключение средств защиты;
-вывод из строя аппаратно-программныхсредстввследствиеошибочных действий;
-накопление данных пользователем информационной системы;
-злонамеренное блокирование данных;
-фальсификация данных;
-несанкционированный доступ персонала ИС к ресурсам;
-компрометация аутентификатора;
-компрометация ключа СКЗИ;
-нарушение функционирования средства защиты;
-перехват в пределах контролируемой зоны внутренними нарушителями;
-угрозы сканирования, направленные на выявление типа или типов используемых, операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
-угрозы выявления паролей по сети;
-угрозы навязывание ложного маршрутасети;
-угрозыподменыдоверенногообъектавсети;
-угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
-угрозы типа «Отказ в обслуживании»;
-угрозы удаленного запуска приложений;
-вторжение в ИСПДн по информационно-телекоммуникационным сетям.

Приложение № 9
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

МАТРИЦА ДОСТУПА
СОТРУДНИКОВ К ЗАЩИЩАЕМЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ ИСПДН

Группа	Уровень доступа к ПДн	Разрешенные действия
Администратор ИСПДн	Полная информация о системном и прикладном ПО ИСПДн. Полная информация о технических средствах и конфигурации ИСПДн. Доступ ко всем техническим средствам обработки информации и данным ИСПДн. Права по конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Администратор информационной безопасности	Права Администратора ИСПДн. Полная информация об ИСПДн. Доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Операторы ИСПДн с правами записи	Права доступа к ПДн по направлениям	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение

Приложение № 10
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

ПРАВИЛА
работы с обезличенными персональными данными в ГБУЗ РБ Бакалинская ЦРБ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила работы с обезличенными персональными данными в ГБУЗ РБ Бакалинская ЦРБ (далее - Правила) разработаны с учетом Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Федеральный закон) и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Правила определяют порядок работы с обезличенными персональными данными в ГБУЗ РБ Бакалинская ЦРБ.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В соответствии с Федеральным законом:

2.1.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

2.1.3. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.2. Администратор безопасности информационных систем персональных данных ГБУЗ РБ Бакалинская ЦРБ и ответственные за организацию обработки персональных данных определяются приказом.

III. СПОСОБЫ И ПОРЯДОК ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обезличивание персональных данных проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения уровня защищенности информационных систем персональных данных ГБУЗ РБ Бакалинская ЦРБ и по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

3.2. Способы обезличивания персональных данных определены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 №996 «Об утверждении требований и методов по обезличиванию персональных данных», а именно:

3.2.1. Уменьшение перечня обрабатываемых сведений.

3.2.2. Замена части сведений идентификаторами.

3.2.3. Понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город).

3.2.4. Деление сведений на части и обработка в разных информационных системах.

3.2.5. Другие способы в соответствии с действующим законодательством.

3.3. Порядок обезличивания:

3.3.1. Руководители структурных подразделений, непосредственно осуществляющие обработку персональных данных, готовят предложения главному врачу ГБУЗ РБ Бакалинская ЦРБ по обезличиванию персональных данных с обоснованием такой необходимости и указанием способа обезличивания.

3.3.2. Главный врач ГБУЗ РБ Бакалинская ЦРБ принимает решение о необходимости обезличивания персональных данных.

3.3.3. Администратор информационных систем персональных данных в ГБУЗ РБ Бакалинская ЦРБ совместно с ответственным за организацию обработки персональных данных осуществляют непосредственное обезличивание персональных данных.

IV. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

4.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

4.2. Обезличенные персональные данные допускается обрабатывать с использованием и без использования средств автоматизации.

4.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

4.3.1. Парольной политики.

4.3.2. Антивирусной политики.

4.3.3. Правил работы со съемными носителями (если они используется).

4.3.4. Правил резервного копирования.

4.3.5. Правил доступа в помещения, где расположены элементы информационных систем.

4.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

4.4.1. Правил хранения бумажных носителей.

4.4.2. Правил доступа к ним и в помещения, где они хранятся.

V. ОТВЕТСВЕННОСТЬ

Ответственные за обработку персональных данных несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 11
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

Типовое обязательство
сотрудника ГБУЗ РБ Бакалинская ЦРБ, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора, о прекращении обработки персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я,

_____

(фамилия, имя, отчество)

_____

(должность)

_____

_____

обязуюсь прекратить обработку персональных данных, ставших известными мне всвязи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта, освобождения меня от замещаемой должности иувольнения с государственной гражданской службы.

В соответствии со статьей 7 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" и другими федеральными законами, мне разъяснена.

"__" _____ 20__ г. _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение № 12
к приказу ГБУЗ РБ Бакалинская ЦРБ
от 09.01.2023 г. № 113

ПАРОЛЬНАЯ ПОЛИТИКА
в отношении к Государственной информационной системы «Региональная информационно-аналитическая система Республики Башкортостан» (ГИС «РМИАС РБ»)

1. Общие сведения

1.1 Настоящая Политика устанавливает требования к порядку выбора, хранения, использования, периодичности смены и другим вопросам, связанным с применением механизмов парольной аутентификации в ГИС «ГИС «РМИАС РБ»».

1.2 Требования настоящей Политики распространяются на всех пользователей ГИС «ГИС «РМИАС РБ»», а также всех прочих лиц (подрядчики, аудиторы и т.п.) в установленном порядке получивших право на доступ к ресурсам ГИС «РМИАС РБ» в соответствии с функциональными обязанностями.

2. Термины и определения

Термин	Определение
Информационная система	совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения бизнес-задач подразделений Компании. В Компании используются различные типы информационных систем для решения производственных, управленческих, учетных и других бизнес-задач.
ГИС «РМИАС РБ»	государственная информационная система Республики Башкортостан, состоящая из комплекса программных и технических средств, баз данных, обеспечивающих информационно-технологическую поддержку функционирования системы здравоохранения Республики Башкортостан, и предназначенную для выполнения в Республике Башкортостан функций регионального фрагмента Единой государственной информационной системы в сфере здравоохранения.
Пользователи ГИС «РМИАС РБ»	работники медицинских организаций (штатные, временные, работающие по контракту и т.п.), администраторы ГИС «РМИАС РБ», а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в ГИС «РМИАС РБ» в установленном порядке.
Пароль пользователя	секретная (известная только данному пользователю) последовательность символов, используемая пользователем для подтверждения своей подлинности (аутентификации) при входе в систему (сеть), а также (в некоторых случаях) для получения доступа к информационным ресурсам.

Учетная запись пользователя	хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа к данным и настройкам. Учетная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п.
Аутентификация	проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
Несанкционированный доступ	доступ к информации, нарушающий установленные правила разграничения доступа.

3. Основные положения

3.1 Пароли для доступа к ГИС «РМИАС РБ» предоставляются пользователям администратором при регистрации этих сотрудников в качестве пользователей ГИС «РМИАС РБ». При получении первоначального пароля от администратора, пользователь обязан произвести смену этого пароля при первом входе в ГИС «РМИАС РБ». В дальнейшем пользователь должен осуществлять смену своих паролей самостоятельно в соответствии с требованиями настоящей Политики.

3.2 Пользователи ГИС «РМИАС РБ» должны производить смену своих паролей не реже, чемраз в три месяца.

3.3 Пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.

3.4 С целью предотвращения несанкционированного доступа к рабочим местам пользователей, а также к ресурсам ГИС «РМИАС РБ» с использованием чужих учетных записей (имен пользователей), пользователи обязаны блокировать экраны своих компьютеров в случае оставления ими своего рабочего места нажатием на компьютерной клавиатуре набора клавиш Ctrl+Alt+Del и далее - кнопки «Блокировать компьютер».

3.5 Все выбираемые пользователями пароли должны отвечать приведенным ниже требованиям:

- Содержать не менее 8 символов.
- Содержать символы, набранные в разных регистрах (a-z, A-Z)
- Помимо букв, содержать также цифры, знаки препинания и/или специальные символы (0- 9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Не являться словом из словаря, сленга, диалекта, жаргона и т.п.
- Не являться персональной информацией (имена членов семьи, адреса, телефоны, даты рождения и т.п.)

3.6 Пользователи могут выбрать легко запоминающиеся пароли, которые в то же время являются трудно угадываемыми для других лиц, если будет выполнено хотя бы одно изследующих условий:

- Несколько слов написаны слитно (такие пароли известны под названием «passphrases»);
- Набор слова на русском языке на английской раскладке клавиатуры

Намеренно неправильное написание слова (но не обычная в данном слове орфографическаяошибка).

4. Обеспечение конфиденциальности паролей

4.1 Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

4.2 Запрещается:

- Сообщать свой пароль кому-либо, включая коллег, руководителей и специалистов службы технической поддержки, по телефону, по электронной почте или какими-либо иными средствами.

- Хранить пароли в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к ним доступ. Например, ни в каких приложениях пользователи не должны выбирать такую опцию конфигурации, как автоматическое сохранение пароля.

Записывать пароли и оставлять эти записи в местах, где к ним могут получить доступ неуполномоченные лица.

- Произносить свой пароль вслух.

- Использовать общие пароли совместно с другими пользователями.

4.3 Примечания:

1. Если кто-либо требует от Вас раскрытия пароля, сошлитесь на настоящую политику или предложите обратиться за разъяснениями в Отдел информационной безопасности ГКУЗ РБМИАЦ по телефону 8(347)246-55-94.

2. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого пользователя.

3. Системным администраторам для выполнения ими своих служебных обязанностей, ни при каких обстоятельствах, не требуется знание паролей пользователей. Для этого у них есть все необходимые полномочия в ИС. В случае необходимости, они произведут смену пароля пользователя и сообщат ему об этом.

5. Контроль

5.1 Общий контроль выполнения требований настоящей Политики осуществляется сотрудниками отдела информационной безопасности ГКУЗ РБ МИАЦ. С целью проверки надежности используемых паролей по согласованию с системными администраторами ими периодически могут осуществляться тестовые «взломы» паролей пользователей. Системные администраторы имеют право принимать участие в проведении подобных проверок. По указанию сотрудников отдела информационной безопасности ГКУЗ РБ МИАЦ, пользователи должны производить смену паролей, не удовлетворяющих критериям надежности, устанавливаемым настоящей Политикой.

5.2 Системные администраторы там, где это возможно, должны настраивать в операционных системах и приложениях следующие параметры парольной политики:

- Минимальная длина пароля – 8 символов;
- Пароль должен отвечать требованиям сложности;
- Максимальный срок действия пароля – 90 дней;
- Минимальный срок действия пароля – 1 день;
- Не повторяемость паролей (хранить 5 предыдущих);
- Использование шифрования при хранении паролей;
- Автоматическая блокировка пользовательских учетных записей после 5 неудачных попыток введения пароля. (Последующая разблокировка пользовательского пароля может производиться только системным администратором).

Системные администраторы также осуществляют настройку на рабочих местах пользователей автоматического блокирования экранов через 15 минут неактивности.

6. Ответственность

6.1 Ответственность за осуществление общего контроля выполнения правил настоящей Политики, а также за поддержание данного документа в актуальном состоянии несет руководитель начальник отдела информационной безопасности ГКУЗ РБ МИАЦ.

6.2 Ответственность за реализацию системными администраторами требований настоящей Политики, возлагается на начальник отдела информационной безопасности ГКУЗ РБ МИАЦ.

6.3 На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования настоящей Политики, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы за неоднократное грубое нарушение правил работы с ГИС «РМИАС РБ».