Приложение № 1
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПРАВИЛА

обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а так же определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки, при наступлении иных законных оснований в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Общие положения

1.1. Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а так же определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки, при наступлении иных законных оснований в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее - Правила) разработаны на основании требований:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Указа Президента РФ от 06.03.1997 №188 "Об утверждении Перечня сведений конфиденциального характера";
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ);
- Федерального закона от 02.05.2006 №59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации";
- Федерального закона от 21.11.2011 №323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";
- Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановления Правительства РФ от 21 марта 2012 г. №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";
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Правила устанавливают порядок обработки персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Госпиталь), процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные

данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Обработка персональных данных должна осуществляться на законной и справедливой основе.

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

1.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

1.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

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

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

1.8. В настоящих Правилах используются следующие основные понятия:

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

- оператор - Госпиталь, самостоятельно или совместно с другими лицами (учреждениями) организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

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

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

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

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

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

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

- конфиденциальность персональных данных - обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не

распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

- использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

- информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

- доступ к информации - возможность получения информации и ее использования;

- обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель;

- под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (оперативные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

- базой данных является представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью объекта информационных технологий.

Иные понятия в данных Правилах используются в значениях, определенных действующим законодательством Российской Федерации, либо их значение дается по тексту.

2. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

2.1. К процедурам, направленным на предотвращение и выявление нарушений законодательства Российской Федерации в отношении обработки персональных данных и устранение таких последствий, относятся:

- осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», (далее - Федеральный закон) и принятым в соответствии с ним нормативным правовым актом;

- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

- ознакомление сотрудников Госпиталя, непосредственно осуществляющих обработку персональных данных, с законодательством Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, и настоящими Правилами.

2.2. Обеспечение безопасности персональных данных достигается, в частности:

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

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

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

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;

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

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

3. Цели обработки персональных данных

3.1. Целями обработки персональных данных в Госпитале являются:

- заключение, исполнение и прекращение гражданско-правовых договоров с гражданами, юридическими лицами, ИП и другими лицами в ситуациях, предусмотренных законодательством Российской Федерации, Рязанской области и Уставом Госпиталя;

- содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами, обеспечение вопросов награждения государственными наградами Российской Федерации, наградами Рязанской области, поощрениями Губернатора Рязанской области, Правительства Рязанской области, поощрениями Рязанской областной Думы, поощрениями руководства Госпиталя;

- обеспечение объективного, всестороннего и своевременного рассмотрения обращений граждан в установленном законом порядке;

- осуществление контроля за сроками исполнения поручений в автоматизированной системе электронного документооборота;

- исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц, единого социального налога, пенсионного законодательства, формирование и передача в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование;

- заполнение первичной статистической документации в соответствии с Трудовым, Налоговым кодексом и Федеральными Законами;

- ведение медицинского учета пациентов, их медицинского обслуживания, диагностики, лечения и профилактики заболеваний; осуществление медицинской деятельности в соответствии с выданной лицензией.

4. Порядок обработки персональных данных субъектов персональных данных, осуществляемой с использованием средств автоматизации, содержание персональных данных

4.1. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем реализации следующих мер:

- в отношении каждой категории персональных данных определяются места хранения персональных данных (материальных носителей) и устанавливается перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- при хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключение несанкционированного доступа к ним.

4.2. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем принятия необходимых правовых, организационных и технических мер или обеспечения их принятия для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.3. Уполномоченными должностными лицами при обработке персональных данных в информационных системах персональных данных должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

4.4. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

4.5. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети «Интернет», не допускается.

4.6. Доступ пользователей (операторов информационной системы) к персональным данным в информационных системах персональных данных должен требовать обязательного прохождения процедуры идентификации и аутентификации.

4.7. Должностными лицами Госпиталя, ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства;

- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- контроль за обеспечением уровня защищенности персональных данных;

- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.8. В случае выявления нарушений порядка обработки персональных данных в информационных системах уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

5. Порядок обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации

5.1. Обработка персональных данных без использования средств автоматизации уполномоченным должностным лицом осуществляется на материальных (бумажных) носителях персональных данных для целей, указанных в настоящих Правилах.

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

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, фамилию, имя, отчество и адрес субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными не имел возможности доступа к персональным данным иных лиц, содержащимся в указанной типовой форме;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.3. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

5.4. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

6. Порядок обработки персональных сотрудников Госпиталя

6.1. Обработка персональных сотрудников Госпиталя (далее - сотрудники) осуществляется с их письменного согласия, которое действует со дня устройства на работу в Госпиталь на время, определяемое законодательством Российской Федерации.

6.2. Лица, уполномоченные на обработку персональных данных, обеспечивают защиту персональных данных от неправомерного их использования или утраты.

6.3. Обработка персональных данных сотрудников осуществляется, как с использованием средств автоматизации, так и без использования таких средств.

6.4. При обработке персональных данных сотрудников лица, уполномоченные на обработку персональных данных, обязаны соблюдать следующие требования:

- объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;
- защита персональных данных сотрудников от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

- передача персональных данных сотрудников не допускается без их письменного согласия, за исключением случаев, установленных федеральными законами. В случае, если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных либо отсутствует письменное согласие на передачу персональных данных, лицо, уполномоченное на обработку персональных данных, вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;

- обеспечение конфиденциальности персональных данных сотрудников, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

- хранение персональных данных должно осуществляться в форме, позволяющей определить сотрудников и иных лиц, являющихся субъектами персональных данных, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели их обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения персональных данных оформляется соответствующим актом;

- опубликование и распространение персональных данных сотрудников допускаются в случаях, установленных законодательством Российской Федерации.

6.5. В целях обеспечения защиты персональных данных сотрудники вправе:

- получать полную информацию о своих персональных данных и способе обработки этих данных (в том числе автоматизированной);

- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных законодательством Российской Федерации;

- требовать внесения необходимых изменений, уничтожения или блокирования соответствующих персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели их обработки;

- обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц.

7. Сроки обработки и хранения персональных данных, порядок их уничтожения при достижении целей обработки или при наступлении иных законных оснований

7.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

7.2. В случае выявления неправомерной обработки персональных данных, оператор в срок, не превышающий 3 рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов

персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7.3. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных, либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.

7.4. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

7.5. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен законодательством Российской Федерации.

Приложение № 2
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПРАВИЛА

рассмотрения запросов субъектов персональных данных, или их представителей в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

I. Общие положения

1. Настоящие Правила рассмотрения запросов субъектов персональных данных, или их представителей в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Правила, Госпиталь) разработаны на основании требований:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ);
- Федерального закона от 02.05.2006 №59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации";
- Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановления Правительства РФ от 21 марта 2012 г. №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";
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

и принятыми в соответствии с ними нормативными правовыми актами.

2. Целью Правил является определение требований к порядку рассмотрения запросов субъектов персональных данных или их представителей в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Госпиталь).

3. В Госпитале, являющимся оператором, обработка персональных данных субъектов персональных данных должна осуществляться на основе принципов, определенных Федеральным законом № 152-ФЗ.

4. В настоящих Правилах термины и определения применяются в том значении, в котором они применяются в Федеральном законе № 152-ФЗ.

II. Информация, предоставляемая по запросу

5. Субъекту персональных данных, или его представителю по запросу предоставляется информация, касающаяся обработки персональных данных Субъекта, в том числе содержащая:

1) подтверждение факта обработки персональных данных;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным, или которым могут

быть раскрыты персональные данные на основании соглашения с оператором или на основании законодательства Российской Федерации;

5) обрабатываемые персональные данные, относящиеся к соответствующему Субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления Субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

8) информацию об осуществленной, или о предполагаемой трансграничной передаче данных;

9) наименование организации, или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена, или будет поручена такому лицу.

6. Сведения, указанные в пункте 5 настоящих Правил, предоставляются Субъекту персональных данных, или его представителю оператором при обращении либо при получении запроса Субъекта персональных данных, или его представителя. Запрос должен содержать:

1) номер основного документа, удостоверяющего личность Субъекта персональных данных, или его представителя;

2) сведения о дате выдачи указанного документа и выдавшем его органе;

3) сведения, подтверждающие участие Субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись Субъекта персональных данных, или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7. В случае, если сведения, указанные в пункте 5 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления Субъекту персональных данных по его запросу, Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 5 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законом № 152-ФЗ, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект персональных данных.

8. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 5 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 7 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос должен содержать обоснование направления повторного запроса.

III. Требования к содержанию запроса

9. Сведения предоставляются Субъекту персональных данных, или его представителю при обращении либо при получении запроса Субъекта персональных данных, или его представителя.

10. Запрос может быть подан на имя главного врача Госпиталя одним из следующих способов:

1) лично;

2) с использованием почтовой связи;

3) с использованием средств электронной связи, посредством направления электронного документа, подписанного электронной подписью, в соответствии с законодательством Российской Федерации.

11. Запрос должен содержать:

1) номер основного документа, удостоверяющего личность Субъекта персональных данных, или его представителя;

2) сведения о дате выдачи указанного документа и выдавшем его органе;

3) сведения, подтверждающие участие Субъекта персональных данных в отношениях с Госпиталем;

4) подпись Субъекта персональных данных, или его представителя.

12. К запросу прилагается копия документа, удостоверяющего личность субъекта персональных данных, документ, подтверждающий полномочия заявителя при обращении представителя субъекта персональных данных (нотариально заверенная доверенность).

IV. Обязанности Госпиталя при рассмотрении запроса

13. Рассмотрение запросов является служебной обязанностью руководителей структурных подразделений Госпиталя, уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных.

14. Прием, первичная обработка, регистрация и доведение до исполнителей поступивших запросов производятся в соответствии с установленным порядком организации работы с документами в Госпитале.

15. Госпиталь обязан сообщить Субъекту персональных данных, или его представителю информацию о наличии персональных данных, относящихся к соответствующему Субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении Субъекта персональных данных, или его представителя либо в течение 30 (Тридцати) дней с даты получения запроса Субъекта персональных данных, или его представителя.

16. Право Субъекта персональных данных, или его представителя на доступ к персональным данным может быть ограничено в соответствии с Федеральным законом № 152-ФЗ.

В случае отказа в предоставлении информации о наличии персональных данных о соответствующем Субъекте персональных данных, или персональных данных Субъекту персональных данных, или его представителю при их обращении либо при получении запроса субъекта персональных данных, или его представителя Госпиталь обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ, или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения Субъекта персональных данных, или его представителя либо с даты получения запроса Субъекта персональных данных, или его представителя.

17. Госпиталь обязан сообщать в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Приложение № 3
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Правила, Госпиталь) разработаны в соответствии с требованиями:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ);
- Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановления Правительства РФ от 21 марта 2012 г. №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";
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

и принятыми в соответствии с ними нормативными правовыми актами.

2. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

3. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям, организовывается проведение периодических проверок условий обработки персональных данных.

4. Проверки осуществляются комиссией, образуемой приказом главного врача Госпиталя, возглавляемой ответственным за организацию обработки персональных данных в Госпитале.

5. Проверки проводятся не реже одного раза в три года на основании утвержденного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям, или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки обеспечивается в течение трех рабочих дней с момента поступления соответствующего заявления.

6. При проведении проверки соответствия обработки персональных данных требованиям к их защите проверяются:

- выполнение правил обработки персональных данных в Госпитале;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

7. Ответственный за организацию обработки персональных данных в Госпитале имеет право:

- запрашивать информацию, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить главному врачу Госпиталя предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить главному врачу Госпиталя предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

8. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Госпитале в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

9. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, главному врачу Госпиталя докладывает ответственный за организацию обработки персональных данных в Госпитале в форме письменного заключения.

Приложение № 4
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПРАВИЛА

работы с обезличенными данными в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Правила работы с обезличенными данными в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Правила, Госпиталь) разработаны в соответствии с требованиями:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ);
- Постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановления Правительства РФ от 21 марта 2012 г. №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";
- Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

и принятыми в соответствии с ними нормативными правовыми актами.

2. В соответствии со статьей 3 Федерального закона № 152-ФЗ под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Способами обезличивания персональных данных, при условиях их дальнейшей обработки являются:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификации;
- обобщение – понижение точности некоторых сведений (например, «место жительства» может состоять из страны, индекса, города, улицы, дома, квартиры, а может быть указан только город);
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

4 Обезличивание персональных данных осуществляется до достижения целей, предусмотренных Федеральным законом № 152-ФЗ.

5. Сотрудники Госпиталя, ответственные за проведение мероприятий по обезличиванию персональных данных, осуществляют обезличивание персональных данных в следующем порядке:

- главный врач принимает решение о необходимости обезличивания персональных данных;
- ответственный за организацию обработки персональных данных проверяет и согласовывает предложения руководителей структурных подразделений Госпиталя по обезличиванию персональных данных, обоснованию такой необходимости и способам обезличивания;
- сотрудники, осуществляющие обработку персональных данных в связи с реализацией должностных обязанностей, осуществляют непосредственное обезличивание персональных данных.

6. Обработка обезличенных персональных данных может осуществляться с использованием средств автоматизации, или без использования таких средств.

7. При обработке обезличенных персональных данных с использованием средств автоматизации должны соблюдаться требования информационной безопасности, в том числе установленные для информационных систем, в которых обрабатываются указанные данные, а также порядок доступа в помещения, в которых расположены информационные системы персональных данных, в целях исключения несанкционированного доступа к обезличенным персональным данным, возможности их несанкционированного уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий в отношении обезличенных персональных данных.

Указанный порядок доступа обеспечивается в том числе:

- запиранием помещения на ключ, в том числе при выходе из него в рабочее время;
- закрытием металлических шкафов и сейфов, где хранятся носители информации, содержащие обезличенные персональные данные, во время отсутствия в помещении работников Госпиталя, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

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

Приложение № 5
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПЕРЕЧЕНЬ

должностей в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», должностные обязанности которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным

1	главный врач
2	заместитель главного врача
3	заведующий отделением
4	главный бухгалтер
5	ведущий бухгалтер
6	бухгалтер
7	заведующий отделом по организационно-методической работе
8	медицинский статистик
9	начальник отдела информации
10	оператор ЭВМ
11	программист
12	ведущий экономист
13	ведущий специалист по кадрам
14	специалист по кадрам
15	врач
16	медицинский психолог
17	главная медицинская сестра
18	старшая медицинская сестра
19	медицинская сестра
20	фельдшер-лаборант

Приложение № 6
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПЕРЕЧЕНЬ

должностей в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в случае обезличивания персональных данных

1	главный врач
2	главный бухгалтер
3	ведущий бухгалтер
4	бухгалтер
5	заведующий отделом по организационно-методической работе
6	медицинский статистик
7	начальник отдела информации
8	оператор ЭВМ
9	программист
10	ведущий экономист
11	ведущий специалист по кадрам
12	специалист по кадрам

Приложение № 7
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

о порядке взаимодействия государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» с уполномоченным органом по защите прав субъектов персональных данных

1. Область действия

1.1. Настоящий документ разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), постановления Правительства Российской Федерации от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» и определяет порядок взаимодействия государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Госпиталь) с уполномоченным органом по защите прав субъектов персональных данных (далее – Уполномоченный орган).

1.2. Перед началом обработки персональных данных Госпиталь уведомляет Уполномоченный орган о своем намерении осуществлять обработку персональных данных.

1.3. Госпиталь вправе осуществлять без уведомления Уполномоченный орган обработку персональных данных:

- обрабатываемых в соответствии с трудовым законодательством;
- полученных Госпиталем в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- сделанных субъектом общедоступными персональных данных;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- обрабатываемых без использования средств автоматизации в соответствии с Федеральными законами, или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

1.4. Уполномоченный орган имеет право:

- запрашивать у Госпиталя информацию, необходимую для реализации своих полномочий и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от оператора уточнения, блокирования или уничтожения недостоверных ли полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований Федерального закона №152-ФЗ «О персональных данных».

1.5. Распределение ролей.

В процессе взаимодействия с Уполномоченный орган принимают участие следующие должностные лица:

- ответственный за организацию обработки персональных данных;

- администраторы ИСПДн Госпиталя.

2. Порядок взаимодействия с Уполномоченным органом

2.1. В случае неполноты или изменения сведений, указанных в уведомлении об обработке персональных данных, а также в случае прекращения обработки персональных данных Госпиталь уведомляет об изменениях Уполномоченный орган в срок, не превышающий десяти рабочих дней с даты возникновения таких изменений, или с даты прекращения обработки персональных данных. Ответственный за организацию обработки персональных данных направляет в адрес Уполномоченный орган Уведомление об изменениях в реквизитах оператора персональных данных.

2.2. Полученные запросы от Уполномоченного органа регистрируются ответственным за организацию обработки персональных данных в Журнале учета запросов уполномоченного органа по защите прав субъектов персональных данных (далее – Журнал учета запросов). В организации разработана и используется определенная форма указанного журнала.

2.3. Ответственный за организацию обработки персональных данных оценивает правомерность полученных запросов в адрес Госпиталя.

2.4. Ответственный за организацию обработки персональных данных в течение тридцати дней с момента получения запроса формирует ответ на запрос, при необходимости запрашивая информацию у администраторов ИСПДн.

2.5. При получении правомерного запроса на исправление выявленных нарушений по распоряжению ответственного за организацию обработки персональных данных администраторы ИСПДн, в которых обрабатываются указанные ПДн, разрабатывают перечень мер по устранению выявленных нарушений и согласуют данный перечень с заинтересованными подразделениями Госпиталя.

2.6. Устранение выявленных нарушений должно быть произведено в срок, не превышающий трех рабочих дней с даты выявления нарушений. По факту устранения нарушений формируется Уведомление об устранении нарушений в порядке обработки ПДн. Ответственный за организацию обработки персональных данных регистрирует уведомление в Журнале учета запросов.

Ответственный за организацию обработки персональных данных направляет уведомление в адрес уполномоченного органа по защите прав субъектов персональных данных заказным письмом, или курьером и прикладывает копию почтовой квитанции об отправке, или копию письма с отметкой о вручении к Журналу учета запросов.

2.7. В случае если обеспечить правомерность персональных данных невозможно, по распоряжению ответственного за организацию обработки персональных данных администраторы ИСПДн, в которых обрабатываются указанные ПДн в срок, не превышающий десяти рабочих дней уничтожают указанные ПДн с составлением соответствующего Акта. Ответственный за организацию обработки формирует уведомление об уничтожении персональных данных, регистрирует уведомление в Журнале учета запросов.

2.8. Ответственный за организацию обработки персональных данных направляет уведомление в адрес субъекта персональных данных и в адрес Уполномоченного органа заказным письмом, или курьером и прикладывает копии почтовые квитанции об отправке, или копии письма с отметкой о вручении к Журналу учета запросов.

2.9. По факту внесения изменений в ПДн на основании запроса уполномоченного органа по защите прав субъектов ПДн, Ответственный за организацию обработки персональных данных формирует уведомление о внесении изменений в персональные данные, регистрирует его в Журнале учета запросов уполномоченного органа по защите прав субъектов персональных данных.

2.10. Ответственный за организацию обработки персональных данных направляет уведомление в адрес субъекта персональных данных и в адрес Уполномоченного органа

заказным письмом, или курьером и прикладывает копии почтовые квитанции об отправке, или копии письма с отметкой о вручении к Журналу учета запросов.

2.11. Возможно проведение взаимодействия с Уполномоченным органом через информационно-коммуникационную сеть Internet (электронный документооборот).

2.12. Официальный сайт Уполномоченного органаявляется дополнительным средством для обеспечения возможности обращений граждан объединений граждан и юридических лиц в Уполномоченный орган.

2.13. Для составления уведомлений от организаций, обрабатывающих персональные данные нужно выйти на сайт Уполномоченного органа по адресу http://pd.rkn.gov.ru/operators-registry/notification/form/.

2.14. После того, как откроется соответствующая форма ее следует заполнить и отправить в информационную систему Уполномоченного органа. После заполнения формы уведомления о намерении осуществлять обработку персональных данных и отправки ее в информационную систему Уполномоченного органа, необходимо распечатать заполненную форму, после чего ее подписать и направить в соответствующий территориальный орган Уполномоченного органа по месту регистрации Госпиталя.

Приложение № 8
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО

работника государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора, прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

ГБУ РО РОКГВВ
(ФИО руководителя)
от (ФИО работника)
должность работника
паспортные данные работника

Я, _____,
(фамилия, имя, отчество)
настоящим добровольно принимаю на себя обязательства:

- в случае моего увольнения все носители персональных данных, которые находились в моем распоряжении в период работы в ГБУ РО РОКГВВ, передать непосредственному руководителю;
- мне известно, что в соответствии с нормативными правовыми актами Российской Федерации в случае прекращения допуска к персональным данным, я не освобождаюсь от взятых обязательств по их неразглашению;
- я предупрежден(а) об административной и уголовной ответственности за разглашение персональных данных, ставших мне известными в связи с исполнением должностных обязанностей;
- нормы статьи 13.11 КОАП РФ, статьи 137 УК РФ мне разъяснены и понятны.

(число, месяц, год) _____ _____
(подпись) (расшифровка подписи)

Приложение № 9
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ТИПОВАЯ ФОРМА

согласия на обработку персональных данных работника государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», а также иных субъектов персональных данных

Я, _____,
(фамилия, имя, отчество)
зарегистрированный(ая) по адресу: _____
_____
паспорт серия _____ № _____, выдан _____
(дата)
_____
(кем выдан)
в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие уполномоченным должностным лицам государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Госпиталь), зарегистрированного по адресу: 390000, г.Рязань, ул. Вознесенская, д. 63, на обработку (любое действие (операцию), или совокупность действий (операций), совершаемых с использованием средств автоматизации, или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение) следующих персональных данных:

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- реквизиты документа, удостоверяющего личность;
- адрес регистрации, фактический адрес проживания;
- реквизиты загранпаспорта;
- семейное положение, состав семьи, сведения о близких родственниках;
- контактные телефоны;
- данные страхового свидетельства обязательного пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния;
- сведения о трудовой деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании, в том числе о послевузовском профессиональном образовании, данные документов об образовании;
- медицинские заключения и результаты обязательных медицинских осмотров;
- сведения о владении иностранными языками;
- информация о наличии или отсутствии судимости;
- сведения о доходах, об имуществе и обязательствах имущественного характера;
- сведения о государственных наградах, иных наградах, знаках отличия, поощрениях;
- фотография.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере трудовых и непосредственно связанных с ними отношений для реализации полномочий, возложенных на Госпиталь действующим законодательством.

После прекращения трудовых отношений с Госпиталем персональные данные будут храниться в Госпитале в течение предусмотренного законодательством Российской Федерации срока хранения документов.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

(число, месяц, год) _____ _____

(подпись) (расшифровка подписи)

Приложение № 10
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ТИПОВАЯ ФОРМА

разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные государственному бюджетному учреждению Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

Мне, _____,
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные уполномоченным лицам государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», определенные статьями 65, 86 Трудового кодекса Российской Федерации и которые субъект персональных данных обязан предоставить в связи с заключением трудового договора. Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений трудовой договор не может быть заключен.

(число, месяц, год) _____ _____
(подпись) (расшифровка подписи)

Приложение № 11
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Фамилия, имя, отчество;
2. Дата и место рождения;
3. Гражданство;
4. Адрес регистрации, фактический адрес проживания;
5. Реквизиты документа, удостоверяющего личность;
6. Реквизиты загранпаспорта;
7. Контактные телефоны;
8. Реквизиты страхового свидетельства обязательного пенсионного страхования;
9. Идентификационный номер налогоплательщика;
10. Реквизиты страхового медицинского полиса обязательного медицинского страхования;
11. Реквизиты свидетельств о государственной регистрации актов гражданского состояния;
12. Сведения о семейном положении, составе семьи, сведения о близких родственниках;
13. Сведения о трудовой деятельности;
14. Сведения о воинском учете и реквизиты документов воинского учета;
15. Сведения об образовании, в том числе о послевузовском профессиональном образовании;
16. Медицинские заключения и результаты обязательных медицинских осмотров;
17. Информация о наличии или отсутствии судимости;
18. Сведения о государственных наградах, иных наградах, знаках отличия, поощрениях;
19. Сведения о доходах, об имуществе и обязательствах имущественного характера;
20. Иные персональные данные в соответствии с нормативными правовыми актами Российской Федерации, необходимые для реализации полномочий государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

Приложение № 12
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПОРЯДОК

доступа в помещения государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», в которых ведется обработка персональных данных

1. Помещения, в которых ведется обработка персональных данных, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

2. Доступ в помещения, в которых ведется обработка персональных данных, имеют следующие лица:

- сотрудники государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Госпиталь), рабочее место которых расположено в данном помещении;

- лица, доступ которым в помещение оформлен письменным разрешением руководителя соответствующего структурного подразделения государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн».

3. Лица, не имеющие доступа в помещения, где обрабатываются персональные данные, имеют право пребывать в указанных помещениях только в присутствии сотрудников Госпиталя, имеющих право доступа в них.

4. Персональные электронно-вычислительные машины, на которых обрабатываются персональные данные, должны размещаться так, чтобы исключить несанкционированный доступ к информации посторонних лиц.

5. Во время отсутствия в помещениях сотрудников двери должны быть закрыты на замок.

6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на руководителей соответствующих структурных подразделений.

Приложение № 13
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ПЕРЕЧЕНЬ

информационных систем персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

№ п/п	Наименование	Информационная система персональных данных, да/нет
1.	Информационная система ГБУ РО РОКГВВ 1С:Бухгалтерия государственного учреждения	да
2.	Информационная система ГБУ РО РОКГВВ 1С:Зарплата и кадры государственного учреждения	да

Приложение № 14
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Ответственный за организацию обработки персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее - ответственный за организацию обработки персональных данных, Госпиталь) должен руководствоваться в своей деятельности Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», нормативными правовыми актами Правительства Российской Федерации, другими нормативными правовыми актами в области защиты персональных данных, настоящей должностной инструкцией.

2. Ответственный за организацию обработки персональных данных обязан:

- организовывать работу по обработке персональных данных в Госпитале в соответствии с действующим законодательством Российской Федерации;
- предоставлять субъекту персональных данных по его просьбе информацию;
- осуществлять внутренний контроль, за соблюдением требований законодательства Российской Федерации при обработке персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения лиц, осуществляющих обработку персональных данных либо имеющих доступ к персональным данным, положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требования к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- хранить в тайне известные им персональные данные, информировать главного врача о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей.

3. При обработке персональных данных ответственному за организацию обработки персональных данных запрещается:

- передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта и т.п.) без использования сертифицированных средств криптографической защиты информации;
- выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные, из здания Госпиталя.

4. Ответственный за организацию обработки персональных данных, виновный в нарушении требований законодательства о защите персональных данных, в том числе допустивший разглашение персональных данных, несет предусмотренную законодательством Российской Федерации ответственность.

Приложение № 15
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

Администратора безопасности информационных систем персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Общие положения

1.1. Инструкция Администратора информационных систем персональных данных (далее – Администратор ИСПДн) в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Инструкция, Госпиталь) определяет функции, права и обязанности Администратора ИСПДн по вопросам обеспечения правильности использования и нормального функционирования ИСПДн, информационной безопасности в ИСПДн.

1.2. Администратор ИСПДн назначается из числа сотрудников госпиталя и отвечает за обеспечение устойчивой работоспособности элементов ИСПДн, правильность использования и нормальное функционирование системы защиты персональных данных.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

2. Должностные обязанности Администратора ИСПДн

2.1. Администратор ИСПДн обязан:

2.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.1.2. Осуществлять учет и периодический контроль за составом и полномочиями пользователей автоматизированных рабочих станций и серверов ИСПДн госпиталя.

2.1.3. Осуществлять оперативный контроль за работой пользователей автоматизированных рабочих станций, анализировать содержимое системных журналов и реагировать на возникающие нештатные ситуации.

2.1.4. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на автоматизированных рабочих местах ИСПДн госпиталя специальных технических средств защиты от несанкционированного доступа.

2.1.5. Осуществлять контроль технических средств, программного обеспечения и средств защиты информации в ИСПДн госпиталя.

2.1.6. Исключать возможность несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах.

2.1.7. Уничтожать (стирать) или обезличивать персональные данные на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

2.1.8. Обеспечивать установку только разрешенного к использованию программного обеспечения и его компонентов, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения автоматизированных рабочих станций и серверов (операционные системы, прикладное и специальное программное обеспечение);
- аппаратных средств ИСПДн;

- аппаратных и программных средств защиты информации.

2.1.9. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.1.10. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.1.11. Обеспечивать функционирование и поддерживать работоспособность средств защиты информации в рамках возложенных на него функций.

2.1.12. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по своевременному восстановлению и выявлению причин, приведших к их отказу работоспособности.

2.1.13. Проводить периодический контроль принятых мер по защите информации в пределах возложенных на него функций.

2.1.14. Обеспечивать контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.1.15. Информировать ответственного за организацию обработки персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.1.16. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей в случае выявления нарушений установленного порядка работы или нарушения функционирования ИСПДн или средств защиты.

2.1.17. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.1.18. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и организациями.

2.1.19. Проводить занятия с сотрудниками по правилам работы на автоматизированных рабочих местах, оснащенных средств защиты информации от несанкционированного доступа, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

2.1.20. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий.

2.1.21. Докладывать ответственному за организацию обработки персональных данных об имевших место попытках несанкционированного доступа к информации и техническим средствам ИСПДн.

2.1.22. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от несанкционированного доступа, установленных на автоматизированных рабочих местах.

2.1.23. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате несанкционированного доступа.

3. Права Администратора ИСПДн

3.1. Администратор ИСПДн имеет право:

3.1.1. Участвовать в анализе ситуаций, касающихся функционирования ИСПДн и расследования фактов несанкционированного доступа.

3.1.2. Требовать прекращения обработки информации в случае нарушения установленного порядка работы или нарушения функционирования средств и систем защиты ИСПДн.

3.1.3. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.1.4. Вносить свои предложения по совершенствованию мер защиты в ИСПДн.

3.2. Администратор ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.

4. Ответственность Администратора ИСПДн

4.1. Администратор ИСПДн несет ответственность:

4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, - в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.1.2. За правонарушения, совершенные в процессе осуществления своей деятельности, - в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3. За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

4.1.4. За разглашение сведений конфиденциального характера, ставших известными ему по роду работы.

4.1.5. На Администратора ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

Приложение № 16
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1.Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователями являются сотрудники государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Госпиталь), участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющие доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, и нормативными документами Госпиталя.

2.Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Правилах обработки персональных данных Госпиталя.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования инструкции по организации парольной защиты

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Госпиталя, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к Администратору безопасности персональных данных Госпиталя.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору безопасности персональных данных Госпиталя.

2.9. Пользователям запрещается:

- разглашать обрабатываемую информацию третьим лицам;
- копировать обрабатываемую информацию на внешние носители без разрешения своего руководителя;

- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с Администратором безопасности персональных данных Госпиталя.

2.10. При отсутствии визуального контроля за АРМ доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию «Блокировка».

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

4. Права и ответственность пользователей ИСПДн

4.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

4.2 Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение № 17
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» при возникновении внештатных ситуаций

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационной системы персональных данных (далее – ИСПДн) государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее - Госпиталь), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

1.3.1. определение мер защиты от прерывания;

1.3.2. определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей Госпиталя, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

1.4.1. системы обеспечения отказоустойчивости;

1.4.2. системы резервного копирования и хранения данных;

1.4.3. системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в три года.

2. Порядок реагирования на аварийную ситуации

2.1. Действия при возникновении аварийной ситуации.

2.1.1. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1 к настоящей инструкции.

2.1.2. В кратчайшие сроки, не превышающие одного рабочего дня, Администратор безопасности ПДн предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. При необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

2.2.1. При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

2.2.2. Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую

доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

2.2.3. Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

2.3. К авариям относятся следующие инциденты:

2.3.1. Отказ элементов ИСПДн и средств защиты из-за:

2.3.1.1. повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

2.3.1.2. сбой системы кондиционирования.

2.4. Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к работоспособности ИСПДн и средств защиты на сутки и более.

2.5. К катастрофам относятся следующие инциденты:

2.5.1. пожар в здании;

2.5.2. взрыв;

2.5.3. просадка грунта с частичным обрушением здания;

2.5.4. массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

3.1.1.1. системы обеспечения отказоустойчивости;

3.1.1.2. системы резервного копирования и хранения данных;

3.1.1.3. системы контроля физического доступа.

3.1.2. Все критичные помещения Госпиталя (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.1.3. Порядок предотвращения потерь информации ИСПДн описан в инструкции по резервированию и восстановлению персональных данных.

3.2. Организационные меры

3.2.1. Должно быть проведено обучение должностных лиц Госпиталя, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

3.2.1.1. оказание первой медицинской помощи;

3.2.1.2. пожаротушение;

3.2.1.3. эвакуация людей;

3.2.1.4. методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

3.2.1.5. выключение оборудования, электричества, водоснабжения, газоснабжения.

3.2.2. Администратор безопасности ПДн должен быть обучен методам частичного и полного восстановления работоспособности элементов ИСПДн.

3.2.3. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телеком и ИТ угрозы	
17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физически разрыв внешних каналов связи

Приложение № 18
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по организации парольной защиты в информационных системах государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1.1. Данная Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных ГБУ РО «Рязанский областной клинический госпиталь для ветеранов войн» (далее – госпиталь, Инструкция), а также контроль за действиями пользователей и обслуживающего персонала ИСПДн госпиталь при работе с паролями.

2. Требования по организации парольной защиты в ИСПДн госпиталя

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн госпиталя и контроль за действиями исполнителей и обслуживающего персонала ИСПДн при работе с паролями возлагаются на Администратора ИСПДн, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

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

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места (АРМ) и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому.

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

2.4. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора ИСПДн. Для генерации "стойких" значений паролей могут применяться специальные программные средства.

2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 месяцев.

2.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри госпиталя и т.п.) должна производиться Администратором ИСПДн после информирования его об этом кадровыми службами и окончания последнего сеанса работы данного пользователя в ИСПДн госпиталя.

2.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри госпиталя и другие обстоятельства) Администратора ИСПДн и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИСПДн госпиталя.

2.8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.2.6 или п.2.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

3. Ответственность при организации парольной защиты в ИСПДн госпиталя

3.1. Ответственность за организацию парольной защиты в ИСПДн госпиталя и установление порядка ее проведения в соответствии с требованиями настоящей Инструкции возлагается на Администратора ИСПДн.

3.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на Ответственного за организацию обработки ПДн в ИСПДн госпиталя, руководителей структурных подразделений госпиталя и пользователей (операторов) ИСПДн госпиталя.

Приложение № 19
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по управлению доступом к персональным данным в информационных системах персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Введение

1.1. Настоящая инструкция предназначена для обеспечения защиты персональных данных (далее – ПДн), содержащихся в информационной системе персональных данных (далее – ИСПДн) государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее - Госпиталь) при разграничении доступа пользователей к ресурсам и информации, содержащейся в ИСПДн.

1.2. Настоящая инструкция определяет порядок действий администратора безопасности и пользователей ИСПДн при разграничении доступа к ресурсам и информации ИСПДн.

2. Разграничение доступа

2.1. Разграничение доступа к ресурсам и информации ИСПДн осуществляет и контролирует администратор безопасности путем настройки программно – технических средств и средств защиты информации (далее – СЗИ) ИСПДн.

3. Порядок доступа без ввода пароля

3.1. Вход в ИСПДн и действия с ресурсами ИСПДн до процедур идентификации и аутентификации разрешен администратору безопасности для восстановления ИСПДн после сбоев и аварий технических средств ИСПДн. Срок действия разрешения заканчивается в момент запуска ИСПДн после восстановления.

3.2. Доступ к ресурсам ИСПДн до момента прохождения процедур идентификации и аутентификации остальным пользователям запрещен.

4. Порядок предоставления удаленного доступа

4.1. Указанные в пункте 4 требования подлежат исполнению только в случае, если предусмотрен доступ к ресурсам ИСПДн с использованием информационно-телекоммуникационной сети Интернет.

4.2. Удаленный доступ пользователей к информационным ресурсам ИСПДн возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью Госпиталя и внесенных в журнал разрешенных устройств удаленного доступа (Приложение №1 к настоящей Инструкции).

4.3. Выдачу, учет, хранение, настройку программного обеспечения, установку программного обеспечения и его обновление, антивирусную защиту технических средств удаленного доступа осуществляет администратор безопасности. Все данные по конфигурации и настройкам должны быть записаны в журнал разрешенных устройств удаленного доступа.

4.4. При настройке средств удаленного доступа к ресурсам ИСПДн администратор безопасности осуществляет возможность удаленного доступа к ресурсам ИСПДн с автоматической аутентификацией средств удаленного доступа.

5. Порядок использования мобильных технических средств

5.1. Указанные в пункте 4 требования подлежат исполнению только в случае, если предусмотрен доступ к ресурсам ИСПДн с использованием мобильных технические средств.

5.2. К мобильным техническим средствам Госпиталя отнесены все переносные технические устройства, на которые может быть записана и с помощью которых может быть осуществлена обработка информации, содержащейся в ИСПДн.

5.3. Все мобильные технические средства Госпиталя должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет администратор безопасности в журнале учета разрешенных мобильных технических средств (Приложение №2 к настоящей Инструкции).

5.4. При передаче мобильных технических средств на ремонт или техническое обслуживание администратор безопасности полностью очищает их от информации, имеющей отношение к ИСПДн.

6. Взаимодействие с внешними информационными системами (внешними пользователями)

6.1. Пользователям внешних информационных систем (внешним пользователям) доступ к ресурсам ИСПДн устанавливает администратор безопасности путем настройки программно – технических средств и СЗИ ИСПДн.

6.2. Администратор безопасности осуществляет процедуру доступа внешних пользователей к ресурсам ИСПДн в соответствии с пунктом 2 настоящей Инструкции.

7. Заключительные положения

7.1. Сотрудники Госпиталя, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение № 1
к инструкции по управлению доступом к персональным данным в информационных системах персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

ЖУРНАЛ
учета разрешенных средств удаленного доступа

20____ год. Листов (_____)

№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ роспись	Дата возврата/ роспись
1	2	3	4	5	6	7
1	*ноутбук Lenovo B590*	*инв. № 1000013*	*исправен*	*А.С. Трифонов*	*01.01.2018 _____ (А.С. Трифонов)*	*12.06.2018 АБ А.С. Трифонов _____*

Лист _____

ПРАВИЛА
по формированию и ведению журнала учета разрешенных средств удаленного доступа

1. Формирование журнала.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.
2. Ведение журнала.
   Перед началом использования журнала на лицевой стороне обложки указывается дата начала ведения журнала и количество листов в журнале.
   Графы журнала заполняются следующим образом:
   - Графа 1 – номер записи по порядку.
   - Графа 2 – наименование оборудования или программного средства (например – ноутбук Lenovo B590.).
   - Графа 3 – инвентарный или серийный номер (например – инв. № 1000013).
   - Графа 4 – указывается название ИСПДн, где используется устройство.
   - Графа 5 – пользователь оборудования или ПО (например – Иванов И.И.).
   - Графа 6 – дата выдачи и подпись пользователя (например – 01.01.2018 _____ Иванов И.И.).
   - Графа 7 – дата возврата оборудования и подпись администратора безопасности (например – 12.06.2018 АБ А.С. Трифонов _____).

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк

Приложение № 2
к инструкции по управлению доступом к персональным данным в информационных системах персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

ЖУРНАЛ
учета разрешенных средств удаленного доступа

20____ год. Листов (_____)

№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ роспись	Дата возврата/ роспись
1	2	3	4	5	6	7
1	*ноутбук Lenovo B590*	*инв. № 1000013*	*исправен*	*А.С. Трифонов*	*01.01.2018 _____ (А.С. Трифонов)*	*12.06.2018 АБ А.С. Трифонов _____*

Лист _____

ПРАВИЛА
по формированию и ведению журнала учета разрешенных мобильных технических средств

1. Формирование журнала.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.
2. Ведение журнала.
   Перед началом использования журнала на лицевой стороне обложки указывается дата начала ведения журнала и количество листов в журнале.
   Графы журнала заполняются следующим образом:
   - Графа 1 – номер записи по порядку.
   - Графа 2 – наименование оборудования (например – ноутбук Lenovo B590.).
   - Графа 3 – инвентарный или серийный номер (например – инв. № 1000013).
   - Графа 4 – указывается название ИСПДн, где используется устройство.
   - Графа 5 – пользователь оборудования (например – Иванов И.И.).
   - Графа 6 – дата выдачи и подпись пользователя (например – 01.01.2018 _____ Иванов И.И.).
   - Графа 7 – дата возврата оборудования и подпись администратора безопасности (например – 12.06.2018 АБ А.С. Трифонов _____).

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

.

Приложение № 20
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по защите машинных носителей персональных данных, используемых в информационной системе персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

Введение

Настоящая инструкция определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей информации в государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Госпиталь).

Машинный носитель информации (далее – МНИ) – это материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде, в том числе персональных данных (далее – ПДн). МНИ делятся на съемные и несъемные носители.

Несъемные МНИ являются частью автоматизированного рабочего места (далее – АРМ) или сервера и в процессе эксплуатации не предполагают демонтаж.

К съемным носителям относятся любые технические устройства, предназначенные для запоминания информации, оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) или считывания с них информации в память АРМ (или сервера).

Учет машинных носителей информации

Все используемые в информационной системе персональных данных Госпиталя (далее – ИСПДн) МНИ подлежат учёту.

Учет, хранение и выдачу носителей информации осуществляет администратор безопасности.

Учет всех видов и типов носителей информации производится в Журнале учета машинных носителей информации (Приложение №1 к настоящей Инструкции).

На несъемную часть носителей ИСПДн наносится уникальный в пределах Госпиталя учетный номер.

Выдача машинных носителей информации

Пользователи ИСПДн получают учтенный носитель от администратора безопасности, для выполнения работ на конкретный срок.

При получении пользователем носителя информации делается соответствующая запись в Журнале учета машинных носителей информации.

По окончании работ или установленного срока использования пользователь ИСПДн сдает носитель информации администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей информации.

Использование и передача машинных носителей информации

На МНИ записываются исключительно ПДн и программные средства обработки ПДн, содержащихся в ИСПДн.

Носители информации, допускающие повторную запись информации, проходят процедуру многократной перезаписи общедоступной информации перед повторным использованием или ремонтом с целью гарантированного уничтожения остаточной информации. Процедуру перезаписи организует и контролирует администратор безопасности.

ПДн, используемые в различных целях, записываются на разные носители.

Вынос учтенных носителей информации за пределы установленных мест обработки ПДн допустим только с письменного разрешения ответственного за организацию обработки ПДн.

Передача носителей, содержащих ПДн, которые обрабатываются в ИСПДн сторонним организациям или третьим лицам производится по приказу главного врача через администратора безопасности. Администратор безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей информации.

Хранение машинных носителей информации

Хранение МНИ осуществляется в условиях, препятствующих несанкционированному ознакомлению с информацией, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

МНИ хранятся в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним.

ЗАПРЕЩАЕТСЯ хранить носители информации на рабочих столах, оставлять их без присмотра, передавать на хранение третьим лицам.

Действия при утрате или порче машинных носителей информации

В случае утраты или порчи пользователем МНИ, содержащих ПДн, которые обрабатываются в ИСПДн, немедленно ставится в известность администратор безопасности. Администратор безопасности вносит соответствующую запись в Журнал учета машинных носителей информации и докладывает об инциденте ответственному за организацию обработки ПДн.

По факту утраты или порчи МНИ ответственным за организацию обработки ПДн проводится служебное расследование в установленном порядке.

Носители, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

Уничтожение машинных носителей информации

Уничтожение МНИ организует администратор безопасности с предоставлением Акта уничтожения машинных носителей информации (Приложение №2 к настоящей Инструкции) ответственному за организацию обработки ПДн. Акт подписывает администратор безопасности.

Уничтожение носителей информации производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе. Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе. Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей Госпиталя.

Ограничения и ответственность

Всем пользователям ИСПДн запрещено использовать учтенные МНИ для личных целей.

Пользователям ИСПДн запрещено передавать носители информации кому-либо, осуществлять учет, хранение и выдачу носителей информации, обрабатываемой в ИСПДн. Передача носителей информации осуществляется в порядке, предусмотренном пунктами 4.5, 4.6 настоящей Инструкции.

Любое взаимодействие (чтение, запись информации, запуск программного обеспечения) между техническими средствами ИСПДн, СЗИ и неучтенными носителями информации запрещено.

В случае выявления фактов утраты, несанкционированного и (или) нецелевого использования учтенных носителей информации, использования неучтенных (личных) носителей информации в ИСПДн назначается служебное расследование. По результату расследования и по представлению ответственного за организацию обработки ПДн, главный врач принимает решение о привлечении пользователя ИСПДн к ответственности согласно нормативным актам Госпиталя и действующему законодательству.

Сотрудники Госпиталя, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Заключительные положения

Пользователи ИСПДн должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции и ознакомлены с Инструкцией до начала работы в ИСПДн.

Приложение № 1
по защите машинных носителей персональных данных, используемых в информационной системе персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

ЖУРНАЛ
учета машинных носителей персональных данных

20____ год. Листов (_____)

Учетный / заводской номер	Наименование (марка) носителя	Вид носителя (съемный /несъемный)	Цель обработки хранимых ПДн	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения съемного носителя и подпись	Дата возврата съемного носителя и подпись администратора	Отметка об уничтожении носителя
1	2	3	4	5	6	7	8	9
инв. № 1000013	*USB flash drive Transcend JF V30/2Gb*	*съемный*	*информационное обеспечение приема граждан в образовательные организации для получения среднего профессионального и высшего образования*	*нет*	*А.С. Трифонов*	*01.01.2018 _____ (А.С. Трифонов.)*	*12.06.2018 _____ (А.С. Трифонов.)*	*уничтожен 20.06.2018*

Лист _____

ПРАВИЛА

по формированию и ведению журнала учета машинных носителей персональных данных

1. Формирование журнала.

1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.

1.2. Обложка журнала изготавливается на отдельном листе.

1.3. Все листы журнала, за исключением листов обложки, нумеруются.

1.4. Все листы журнала, вместе с обложкой сшиваются.

2. Ведение журнала.

2.1. Перед началом использования журнала на лицевой стороне обложки указывается дата начала ведения журнала и количество листов в журнале.

2.2. Графы журнала заполняются следующим образом:

2.2.1. Графа 1 – учетный или заводской номер носителя (например – инв. № 1000013).

2.2.2. Графа 2 – наименование носителя (например – USB flash drive Transcend JF V30/2Gb.).

2.2.3. Графа 3 – указывается съемный или несъемный носитель (например – съемный).

2.2.4. Графа 4 – указывается цель обработки ПДн, записываемых на носитель.

2.2.5. Графа 5 – для несъемных носителей указывается АРМ пользователя.

2.2.6. Графа 6 – ФИО пользователя.

2.2.7. Графа 7 – дата получения носителя и подпись пользователя безопасности.

2.2.8. Графа 8 – дата возврата носителя и подпись администратора безопасности

2.2.9. Графа 9 – отметку делает администратор безопасности после уничтожения носителя.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 2
по защите машинных носителей персональных данных, используемых в информационной системе персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

АКТ
уничтожения носителей персональных данных

Комиссия в составе:
Председатель комиссии _____

члены комиссии _____
_____
_____
_____

настоящим актом подтверждает, что:

1. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____

2. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____

3. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____

4. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____

уничтожены по причине их неработоспособности путем разрушения их целостности
"____" _____ 20_ г.

Председатель комиссии

_____ _____
(подпись) (инициалы, фамилия)

Члены комиссии

_____ _____
(подпись) (инициалы, фамилия)
_____ _____
(подпись) (инициалы, фамилия)
_____ _____
(подпись) (инициалы, фамилия)
_____ _____
(подпись) (инициалы, фамилия)

Приложение № 21
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по антивирусной защите в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Общие положения

1.1. Настоящая Инструкция предназначена для Администратора информационных систем персональных данных (далее - ИСПДн), Ответственного за организацию обработки персональных данных (далее - ПДн) в ИСПДн и пользователей, эксплуатирующих ИСПДн, государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Инструкция, Госпиталь).

1.2. Инструкция устанавливает требования и ответственность Администратора ИСПДн, Ответственного за организацию обработки ПДн и пользователей ИСПДн при организации защиты персональных данных от воздействия вредоносных компьютерных вирусов.

1.3. Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИСПДн Госпиталя.

2. Требования по обеспечению антивирусной защиты в ИСПДн Госпиталя

2.1. Требования к порядку организации антивирусной защиты.

2.1.1. Для организации антивирусной защиты в ИСПДн Госпиталя допускаются к использованию только лицензионные антивирусные средства.

2.1.2. Обновление антивирусных программных средств осуществляется в установленном порядке, но не реже чем два раза в месяц Администратор ИСПДн должен производить обновление антивирусных баз, получая их из официальных источников. Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляются Ответственным за организацию обработки персональных данных в ИСПДн с привлечением (при необходимости) Администратора ИСПДн и/или специалистов лицензированной организации.

2.1.3. Должностные лица не должны допускать использования в ИСПДн программного обеспечения (ПО) и данных, не связанных с выполнением должностных обязанностей.

2.2. Требования к порядку проведения антивирусного контроля.

2.2.1. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором ИСПДн на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения автоматизированного рабочего места (далее - АРМ) (локальной вычислительной сети) должна быть выполнена антивирусная проверка:

- на защищаемых серверах и АРМ - Администратором ИСПДн;
- на других серверах и АРМ, не требующих защиты, - лицом, установившим (изменившим) программное обеспечение, в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

2.2.2. При загрузке компьютера должен проводиться антивирусный контроль в автоматическом режиме. Порядок и периодичность расширенного антивирусного контроля и других необходимых антивирусных проверок определяется Администратором ИСПДн на этапе планирования мероприятий установленным порядком (не реже одного раза в месяц и при необходимости в случае появления подозрении в заражении вирусной программой).

2.2.3. Обязательному дополнительному антивирусному контролю подлежит любая информация на съемных машинных носителях информации, поступающая для обработки в

ИСПДн Госпиталя. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель информации). Руководители структурных подразделений несут персональную ответственность за предоставление съемных машинных носителей на дополнительный антивирусный контроль Администратору ИСПДн Госпиталя.

2.2.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИСПДн самостоятельно или вместе с Администратором ИСПДн должен провести внеочередной антивирусный контроль своей рабочей станции для определения ими факта наличия или отсутствия компьютерного вируса.

2.2.5. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИСПДн обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя и Администратора ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе Администратору ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;
- по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность при организации антивирусной защиты в ИСПДн Госпиталя

3.1. Ответственность за организацию антивирусной защиты в ИСПДн Госпиталя и установление порядка ее проведения в соответствии с требованиями настоящей Инструкции возлагается на Администратора ИСПДн.

3.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на Ответственного за организацию обработки ПДн в ИСПДн Госпиталя, руководителей структурных подразделений Госпиталя и пользователей (операторов) ИСПДн Госпиталя.

Приложение № 22
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по контролю защищенности персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Введение

Настоящая инструкция определяет порядок выявления, анализа и устранения уязвимостей, недостатков программного обеспечения, аппаратных средств, организационно-технических недостатков в информационных системах персональных данных (далее – ИСПДн) государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» при контроле защищенности персональных данных, обрабатываемых в ИСПДн.

2. Выявление анализ и устранение уязвимостей

2.1. Уязвимость – это недостаток ИСПДн или системы защиты персональных данных (далее – ПДн), который может привести к реализации угрозы безопасности персональных данных.

2.2. Периодичность плановых процедур выявления, анализа и устранения уязвимостей ИСПДн составляет 1 (один) год. Внеплановые процедуры выявления, анализа и устранения уязвимостей ИСПДн проводят по распоряжению ответственного за организацию обработки ПДн в случае необходимости. Необходимость внеплановой процедуры выявления и устранения уязвимостей определяет ответственный по организации обработки ПДн.

2.3. В ИСПДн должно осуществляться выявление и устранение следующих типов уязвимостей:

- недостатки и (или) ошибки программного обеспечения ИСПДн и ее системы защиты информации (далее – СИЗИ);
- недостатки аппаратных средств ИСПДн, в том числе аппаратных средств защиты информации;
- организационно-технические недостатки.

2.4. Мероприятия по выявлению, анализу и устранению уязвимостей организует ответственный за организацию обработки ПДн. Непосредственным исполнителем мероприятий по выявлению, анализу и устранению уязвимостей ИСПДн является администратор безопасности ИСПДн.

3. Недостатки программного обеспечения

3.1. Проверка конфигурации и настроек программно – технических средств ИСПДн и их систем защиты информации на соответствие требованиям эксплуатационной документации и требований к защите ПДн.

3.2. Проверка наличия и сроков действия лицензий на установленное программное обеспечение ИСПДн.

3.3. Проверка наличия последних обновлений используемого программного обеспечения ИСПДн:

- проверка соответствия обновлений версиям программного обеспечения, установленного в ИСПДн и системе защиты информации;
- проверка обновлений вирусных баз;
- проверка обновлений баз решающих правил для средств обнаружения вторжений (при использовании средств обнаружения вторжений);
- проверка обновлений баз признаков уязвимостей.

3.4. Устранение обнаруженных недостатков на основании своих полномочий осуществляют администратор безопасности ИСПДн.

4. Недостатки аппаратных средств

4.1. К недостаткам аппаратных средств, используемых в ИСПДн, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

4.2. При выявлении недостатков аппаратных средств проверяют:

- техническое состояние аппаратных средств;
- наличие сертификатов соответствия на примененные в ИСПДн и ее системе защиты информации аппаратные средства;
- наличие у поставщиков обновленных версий аппаратных средств, примененных в ИСПДн и системе защиты информации;
- конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

4.3. Проверку осуществляет администратор безопасности ИСПДн.

4.4. Обнаруженные в ходе проверки отклонения от конфигурации ИСПДн устраняет администратор безопасности ИСПДн. При обнаружении аппаратных средств с низкой надежностью, частыми выходами из строя администратор безопасности ИСПДн принимает меры по ремонту или замене этих аппаратных средств.

5. Организационно – технические недостатки

5.1. Проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите ПДн, обрабатываемых в ИСПДн.

5.2. Проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД).

5.3. Проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям.

5.4. Проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям.

5.5. Проверка соответствия выполнения правил разграничения доступа к ПДн и ресурсам ИСПДн принятым требованиям.

5.6. Проверка соответствия полномочий пользователей принятым требованиям.

5.7. Проверка наличия документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей.

5.8. Проверка состояния физической защиты ИСПДн (средства охраны и физического доступа в контролируемых зонах ИСПДн).

5.9. Проверки организует ответственный за организацию обработки ПДн с участием администратора безопасности ИСПДн.

6. Заключительные положения

6.1. Сотрудники Госпиталя, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение № 23
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по защите технических средств информационных систем персональных данных в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Введение

1.1. Настоящая инструкция предназначена для обеспечения защищенности персональных данных (далее – ПДн), обрабатываемых в информационной системе персональных данных (далее – ИСПДн) государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее - Госпиталь).

1.2. Настоящая инструкция определяет порядок действий администратора безопасности ИСПДн и пользователей ИСПДн при защите технических средств ИСПДн, в том числе технических средств системы защиты информации.

2. Определение границ контролируемой зоны

2.1. Границами контролируемой зоны ИСПДн являются внешние границы стен помещений (включая окна и двери), в которых размещено оборудование ИСПДн и ее средства защиты информации (далее – СЗИ).

2.2. Перемещение стационарного оборудования ИСПДн и СЗИ за границу контролируемой зоны не допускается.

2.3. Несанкционированный вынос за границу контролируемой зоны учтенных машинных носителей, мобильных технических средств запрещен.

2.4. Несанкционированный внос пользователями ИСПДн неучтенных машинных носителей, мобильных технических средств запрещен.

3. Доступ в контролируемую зону

3.1. На период обработки защищаемых ПДн в помещениях, где размещено оборудование ИСПДн и СЗИ, могут находиться только пользователи, допущенные к обработке персональных данных.

3.2. Нахождение в помещениях контролируемых зон других лиц (например, для проведения необходимых профилактических или ремонтных работ, посетителей) возможно только в присутствии пользователя, допущенного к обработке персональных данных.

3.3. Организацию доступа в помещения контролируемых зон ИСПДн осуществляют пользователи, допущенные к обработке персональных данных, руководители данных структурных подразделений.

4. Правила размещения устройств вывода информации

4.1. При размещении в помещениях контролируемых зон технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации.

4.2. Выполнение требований к размещению устройств вывода информации в контролируемых зонах обеспечивают пользователи, допущенные к обработке персональных данных, руководители данных структурных подразделений..

5. Защита каналов связи

5.1. Технические средства (кабельные разъемы, маршрутизаторы, сетевой экран и т.п.) для подключения ИСПДн к каналам связи, выходящими за пределы контролируемой зоны, должны быть размещены в пределах контролируемой зоны.

5.2. Расположение указанных технических средств и физический доступ к ним контролирует администратор безопасности ИСПДн.

6. Заключительные положения

6.1. Сотрудники Госпиталя, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение № 24
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по резервированию и восстановлению персональных данных в информационной системе персональных данных

1. Общие положения

1.1. Инструкция по резервированию и восстановлению массивов персональных данных в информационных системах персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Инструкция, Госпиталь) определяет порядок резервирования и восстановления содержащих персональные данные (далее - ПДн) баз данных ИСПДн госпиталя.

1.2. Настоящая Инструкция подготовлена с целью обеспечения:

- возможности восстановления содержащих ПДн баз данных (далее - БД) при возникновении такой необходимости;
- целостности и конфиденциальности данных, хранящихся на резервных носителях.

1.3. В настоящей Инструкции регламентируются мероприятия по настройке компонент резервного копирования БД, резервированию БД, хранению носителей резервных копий, выводу из эксплуатации носителей резервных копий, восстановлению БД.

1.4. Имеются следующие типы резервных копий БД:

Тип	Периодичность резервирования	Способ резервирования	Место хранения	Срок хранения
Первый тип	1 раз в сутки	автоматически	На несъемных жестких магнитных дисках	30 суток
Второй тип	1 раз в неделю	вручную	На съемных жестких магнитных дисках	5 недель
Третий тип	1 раз в месяц	вручную	На съемных жестких магнитных дисках	На время существования оператора

2. Настройка компонент резервного копирования БД

2.1. Администратор ИСПДн настраивает резервирование БД на несъемные жесткие диски.

2.2. Резервирование БД осуществляется средствами управления баз данных или средствами установленной операционной системы. Для этого необходимо сделать настройки конфигурации для интерактивного резервирования и выполнить резервирование.

2.3. Для автоматического резервирования необходимо назначить задание Мастеру планирования заданий операционной системы с указанием соответствующего времени.

3. Резервирование БД на внешние носители

3.1. Администратор ИСПДн регистрирует внешний носитель для хранения резервной копии БД в соответствующем журнале.

3.2. Администратор ИСПДн записывает резервную копию БД на соответствующий носитель. Запрещено записывать резервную копию БД на внешние носители, не зарегистрированные должным образом, как носители для хранения резервных копий БД.

3.3. Администратор ИСПДн проверяет качество записанной резервной копии БД.

3.4. Администратор ИСПДн помещает внешний носитель резервной копии БД в защищенное хранилище.

4. Хранение внешних носителей резервных копий БД

4.1. Хранение внешних носителей резервных копий БД осуществляет Администратор ИСПДн.

4.2. Должно быть обеспечено надежное хранение всех внешних носителей резервных копий БД в защищенных хранилищах.

4.3. По истечении срока хранения резервной копии БД данная копия подлежит уничтожению. При выходе из строя носителя резервных копий БД Администратор ИСПЛн осуществляет его вывод из эксплуатации. При этом факт вывода из эксплуатации регистрируется в соответствующем журнале. По решению Администратора ИСПДн исправный внешний носитель резервных копий БД может использоваться повторно. При невозможности его эксплуатации, Администратор ИСПДн осуществляет его физическое уничтожение, о чем делается отметка в соответствующем журнале.

4.4. Несъемные жесткие магнитные диски, предназначенные для хранения резервных копий БД первого типа, выводятся из эксплуатации путем уничтожения всей защищаемой информации специальными средствами гарантированного уничтожения или путем двукратной записи произвольной информации в освобождаемые области памяти, или путем их физического уничтожения.

5. Восстановление БД

5.1. Набор исходных данных, необходимых для восстановления БД:

Документ	Ответственный за хранение	Ответственный за использование
Пароль учетной записи администратора операционной системы	Администратор ИСПДн	Администратор ИСПДн
Резервная копия БД в виде набора файлов на внешнем носителе	Администратор ИСПДн	Администратор ИСПДн
Лицензии установленных операционных систем	Администратор ИСПДн	Администратор ИСПДн
Дистрибутивы операционной системы и средств защиты информации	Администратор ИСПДн	Администратор ИСПДн
Лицензии на средства защиты информации	Администратор ИСПДн	Администратор ИСПДн
Инструкция по резервированию и восстановлению массивов персональных данных в ИСПДн	Администратор ИСПДн	Администратор ИСПДн

5.2. Для восстановления БД используется наиболее актуальная резервная копия БД 1 типа. Проверку возможности использования данной резервной копии БД для восстановления БД осуществляет Администратор ИСПДн.

5.3. При невозможности использования резервных копий БД 1 типа используется наиболее актуальная резервная копия БД 2 типа.

5.4. При невозможности использования резервных копий БД 2 типа используется наиболее актуальная резервная копия БД 3 типа.

5.5. Восстановление БД осуществляет Администратор ИСПДн. Восстановление БД производится в соответствии с эксплуатационной и технической документацией на соответствующую систему управления БД.

Приложение № 25
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по обращению с криптосредствами, предназначенными для защиты персональных данных, обрабатываемых в информационных системах персональных данных государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. Общие положения

1.1. Инструкция по обращению с криптосредствами, предназначенными для защиты персональных данных, обрабатываемых в ИСПДн государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – Инструкция, Госпиталь) регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты персональных данных, обрабатываемых с использованием средств автоматизации.

1.2. Настоящая Инструкция подготовлена в соответствии с «Типовыми требованиями 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», утв. руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/6/6-622 (далее – Типовые требования).

1.3. Под криптосредством в настоящей Инструкции понимается шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

1.4. К криптосредствам (шифровальным, криптографическим средствам) относятся:

- средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;
- средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;
- средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;
- средства изготовления ключевых документов (независимо от вида носителя ключевой информации);
- ключевые документы (независимо от вида носителя ключевой информации).

1.5. В настоящей Инструкции используются следующие понятия и определения:

- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

- доступ к информации - возможность получения информации и ее использования;

- закрытый ключ – криптоключ, который хранится пользователем системы в тайне;

- информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

- информационная система персональных данных - информационная система, представляющая 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;

- ключевой документ - физический носитель определенной структуры, содержащий криптоключи;

- компрометация криптоключа - утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации;

- контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения;

- конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

- криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

- модель нарушителя - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности;

- модель угроз - перечень возможных угроз;

- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

- пользователь криптосредства - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования;

- распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в

информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним;

- средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.6. Для обеспечения безопасности персональных данных при их обработке в ИСПДн Госпиталя должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.7. Класс криптосредства определяется в соответствии «Методическими рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утв. руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/5-144.

2. Организационная структура

2.1. Безопасность обработки персональных данных (далее ПДн) в информационной системе персональных данных Госпиталя с использованием криптосредств организует и обеспечивает Администратор ИСПДн.

3. Кадровая политика

3.1. Пользователи криптосредств допускаются к работе с ними, только после ознакомления с настоящей Инструкцией.

4. Обязанности пользователей криптосредств

4.1. Пользователи криптосредств обязаны:

- не нарушать конфиденциальность закрытых ключей;
- не допускать снятие копий с ключевых документов, содержащих закрытые ключи;
- не допускать вывод закрытых ключей на дисплей (монитор) ПЭВМ или принтер;
- не допускать записи на ключевой документ посторонней информации;
- не допускать установки ключевых документов в ПЭВМ не предназначенные для работы с ними;
- обеспечить конфиденциальность информации о криптосредствах, других мерах защиты;
- не нарушать конфиденциальность защищаемых ПДн;
- точно соблюдать требования к обеспечению безопасности ПДн, требования к обеспечению безопасности криптосредств и ключевых документов к ним;
- надежно хранить эксплуатационную и техническую документацию к криптосредствам, ключевые документы, носители дистрибутивов криптосредств, бумажные и машинные носители ПДн;
- сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;
- своевременно выявлять и сообщать ответственному за организацию обработки персональных данных в информационных системах персональных данных Госпиталя о ставших известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним, защищаемых ПДн;
- немедленно уведомлять ответственного за организацию обработки персональных данных в информационных системах персональных данных Госпиталя и принимать меры по

предупреждению нарушения конфиденциальности защищаемых ПДн при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности ПДн.

5. Обязанности пользователей криптосредств

5.1. Ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель информации.

5.2. Передача ключевых документов допускается только между пользователями криптосредств и Администратором ИСПДн Госпиталя под роспись в соответствующем журнале поэкземплярного учета. Аналогичная передача между пользователями криптосредств осуществляется с санкции Администратора ИСПДн Госпиталя.

5.3. Учет эксплуатационной и технической документации к криптосредствам/

- эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету;
- все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под роспись;

5.4. Распространение ключевых документов:

- ключевые документы получаются лично владельцем криптографического ключа в удостоверяющем центре или Администратором ИСПДн Госпиталя по доверенности выданной владельцем криптографического ключа.

5.5. Плановая смена ключевых документов:

- заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

5.6. Внеплановая смена ключевых документов:

- криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

5.7. Уничтожение ключевых документов:

- ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются Администратору ИСПДн Госпиталя, или по его указанию уничтожаются на месте пользователями криптосредств;
- уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого носителя;
- бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин;
- ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 суток после вывода их из действия (окончания срока действия);
- пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом Администратора ИСПДн Госпиталя.

5.8. Уничтожение эксплуатационной и технической документации к криптосредствам:

- эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин.

6. Техническое обслуживание криптосредств

6.1. Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

6.2. На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае по согласованию с Администратором ИСПДн Госпиталя необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

7. Организация режима помещений

7.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность ПДн, криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в режимных помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.2. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

7.3. Двери помещений должны закрываться на замок. Правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливается ответственным за организацию обработки персональных данных в информационных системах персональных данных Госпиталя.

8. Порядок доступа к хранилищам

8.1. Криптосредства, эксплуатационная и техническая документация к криптосредствам, ключевые документы хранятся в металлических хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

8.2. При утрате ключа от хранилища замок данного хранилища необходимо заменить. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Об утрате ключа сотрудник должен немедленно оповестить ответственного за организацию обработки персональных данных в информационных системах персональных данных Госпиталя. Порядок хранения документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за организацию обработки персональных данных в информационных системах персональных данных госпиталя;

9. Контроль безопасности криптосредств

9.1. Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на Администратора ИСПДн Госпиталя в пределах его полномочий.

10. Ответственность за нарушение требований

10.1. Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

10.2. Администратор ИСПДн Госпиталя несет ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки ПДн с использованием криптосредств лицензионным требованиям и условиям, эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

Приложение № 26
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЯЗАНСКОЙ ОБЛАСТИ
«РЯЗАНСКИЙ ОБЛАСТНОЙ КЛИНИЧЕСКИЙ ГОСПИТАЛЬ ДЛЯ ВЕТЕРАНОВ ВОЙН»

ЖУРНАЛ

ПОЭКЗЕМПЛЯРНОГО УЧЕТА СКЗИ, ЭКСПЛУАТАЦИОННОЙ И ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ К НИМ, КЛЮЧЕВЫХ ДОКУМЕНТОВ

Начат: «____»_____ 20___г.

Окончен: «___»_____ 20___г.

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

ВСЕГО прошито, пронумеровано
и скреплено печатью

_____ (_____) листов
цифрами прописью

_____ /_____/
подпись ФИО

«___» _____20____г.

Инструкция по ведению журнала

Настоящий журнал разработан в соответствии с формой, утвержденной Приказом ФАПСИ от 13.07.2001 №152 (Приложение №2).

Настоящий журнал введен в действие в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», поскольку для защиты информации в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» применяются криптографические средства защиты информации.

В графе **«Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов»** указывается наименование СКЗИ, например «ViPNet Client 4», а также наименование имеющейся эксплуатационной и технической информации, например «Формуляр», «Руководство пользователя». Здесь же указываются названия ключевых документов. Под «ключевым документом» подразумевается физический носитель ключевой информации с записанной на него ключевой информацией, например электронный ключ eToken или RuToken, дискета, компакт-диск. В случае, если ключевая информация хранится на жестком диске, указывается серийный номер тома диска, который можно получить, выполнив команду dir в командной строке Windows.

В графе **«Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов»** указываются серийные номера СКЗИ, а также номера имеющейся документации при наличии. Серийные номера СКЗИ указаны на самих СКЗИ и/или в формулярах.

В графе «Номера экземпляров (криптографические номера) ключевых документов» указываются номера экземпляров ключевых документов. Как правило, ключевые документы издаются в единственном экземпляре.

В графе **«От кого получены или ФИО ОКЗ, изготовившего ключевые документы»** указывается название организации-распространителя криптографических средств (лицензиата ФСБ), например: «ООО «Информационный центр». В случае, если ключевые документы изготовлены органом криптографической защиты (ОКЗ) самостоятельно, указывается ФИО сотрудника, изготовившего ключевые документы.

В графе **«Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении»** указываются дата и номер сопроводительного письма, которое сопровождало передачу СКЗИ. В случае, если ключевые документы изготовлены органом криптографической защиты (ОКЗ) самостоятельно, в этой графе сотрудник, изготовивший ключевые документы, ставит свою подпись.

В графе **«ФИО пользователя СКЗИ»** указываются Фамилия Имя и Отчество (инициалы) сотрудника, использующего данный экземпляр СКЗИ (ключевого документа).

В графе **«Дата и расписка в получении»** указывается дата получения СКЗИ сотрудником и ставится его подпись.

В графе **«ФИО сотрудника ОКЗ, установившего СКЗИ»** указывается Фамилия и инициалы сотрудника ОКЗ, производившего установку (инсталляцию) криптографического средства.

В графе **«Дата установки и подписи лиц»** указывается дата установки (инсталяции) СКЗИ и лица, производившие установку ставят свои подписи.

В графе **«Номера ТС, в которые установлено СКЗИ»** указываются серийные или инвентарные номера технических средств (компьютеров, моноблоков, ноутбуков и т. д.), на которые было установлено СКЗИ.

В графе **«Дата уничтожения»** указывается дата уничтожение ключевых носителей и/или ключевых документов.

В графе **«ФИО сотрудника, уничтожившего (изъявшего) СКЗИ»** ставится ссылка на акт уничтожения, в котором указаны ФИО председателя и членов комиссии по уничтожению.

В графе **«Номер акта об уничтожении»** указывается номер и дата акта уничтожения СКЗИ.

Приложение № 27
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

ИНСТРУКЦИЯ

по контролю эффективности состояния системы защиты информации в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

Обозначения и сокращения

АРМ – автоматизированное рабочее место
АС – автоматизированная система
ВТСС – вспомогательные технические средства и системы
ИБ – информационная безопасность
ЛВС – локальная вычислительная сеть
Госпиталь – государственное бюджетное учреждение Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»
НСД – несанкционированный доступ
ОТСС – основные технические средства и системы
ТКУИ – технические каналы утечки информации
ТС – технические средства АС

1. Общие положения

1.1. Настоящая Инструкция относится к основным организационно-распорядительным документам в области безопасности информации в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее - Госпиталь) и разработана в соответствии с требованиями «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282, Постановления Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и других нормативных правовых актов в области безопасности информации.

1.2. В настоящей Инструкции определен порядок организации и осуществления контроля состояния защиты информации в информационных системах Госпиталя.

1.3. Настоящая Инструкция разработана с целью своевременного выявления и предотвращения:

– хищения технических средств и носителей информации;

– нарушения заданных характеристик безопасности информации (конфиденциальность, целостность, доступность и другие);

– от действий в отношении информации, не предусмотренных установленными правилами и требованиями, приводящих, в том числе к уничтожению, искажению, модификации (подделки), копированию, блокированию информации;

– преднамеренных программно-технических воздействий на информацию, вызывающих нарушение ее целостности или работоспособности объектов информационных технологий и средств защиты информации;

– утечки информации по техническим каналам.

1.4. Контроль состояния защиты информации включает в себя:

– контроль организации защиты информации;

– контроль эффективности защиты информации.

1.4.1. Контроль организации защиты информации заключается в проверке соответствия организации, наличия и содержания внутренних организационных распорядительных документов требованиям законодательных актов и нормативных

правовых актов в области защиты информации. Целью контроля организации защиты информации является:

– оценка полноты выполнения законодательных актов Российской Федерации, нормативных методических документов уполномоченных органов в области обеспечения безопасности (ФСБ России), уполномоченного органа в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России) и уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) и требований организационно-распорядительных документов в области безопасности информации;

– установление соответствия принятых в Госпитале требований по защите информации;

– определение обоснованности и соответствия принятых организационных мер установленным требованиям в области безопасности информации;

– оценка полноты и качества разработки внутренних организационных распорядительных документов Госпиталя в области безопасности информации.

1.4.2. Контроль эффективности защиты информации заключается в проверке соответствия выполненных мероприятий по защите информации требованиям в области безопасности информации. Целью контроля эффективности защиты информации является проверка:

– отсутствия утечки информации по техническим каналам;

– отсутствия НСД к информации;

– отсутствия предпосылок к совершению НСД (в том числе искажения и модификации (подделки) информации);

– отсутствия возможностей хищения технических средств и носителей информации;

– отсутствия возможностей преднамеренных программно-технических воздействий на информацию, вызывающих нарушение ее целостности или работоспособности объектов информационных технологий и средств защиты информации.

1.5. Оценка состояния защиты информации осуществляется по критериям, учитывающим всю совокупность принятых организационных и технических мероприятий.

1.5.1. Оценка принятых технических мер защиты информации производится по действующим методикам с применением поверенной контрольно-измерительной аппаратуры и сертифицированных программных тестовых средств контроля (контроль защищенности конфиденциальной информации от утечки по техническим каналам, от НСД к информации, модификации информации в средствах и системах информационных технологий).

1.5.2. Контроль защищенности конфиденциальной информации от утечки по техническим каналам, от НСД к информации, модификации информации в средствах и системах информационных технологий является лицензируемым видом деятельности.

1.5.3. Защита информации считается эффективной, если все принятые меры соответствуют установленным требованиям и нормам.

1.6. Контроль состояния защиты информации в Госпитале в пределах установленных полномочий осуществляют:

– ФСТЭК России;

– ФСБ России;

– Роскомнадзор;

– Администратор ИСПДн Госпиталя.

1.6.1. Контроль состояния защиты информации может быть осуществлен прокуратурой.

2. Виды и методы контроля эффективности,рекомендации по его проведению

2.1. Контрольные мероприятия подразделяются по:

– способу организации;

– составу проверочной комиссии.

2.1.1. По способу организации контрольные мероприятия бывают:

– плановые;

– внеплановые.

2.1.1.1. Планирование контрольных мероприятий осуществляется на год и отражается в годовых планах организационных и технических мероприятий по защите информации в Госпитале, утверждаемых Главным врачом. Методика формирования плана организационных и технических мероприятий по защите информации и перечень включаемых в него рекомендуемых мероприятий размещены в Приложении 1.

2.1.1.2. Плановые контрольные мероприятия осуществляются путем проведения периодического и постоянного контроля.

2.1.1.3. Периодический контроль:

– проводится ежегодно в сроки, установленные в утвержденном плане организационных и технических мероприятий по защите информации;

– осуществляется с целью обеспечения систематического наблюдения за состоянием системы защиты информации;

– проводится выборочно (применительно к отдельным темам работ, структурным подразделениям или всему Госпиталю) в части выполнения организационных мероприятий по защите информации;

– проводится ответственным за организацию обработки персональных данных в Госпитале, администратором ИСПДн Госпиталя, а также руководителями структурных подразделений Госпиталя, в части проверки целостности и неизменности информации в информационных системах, с которыми они работают.

2.1.1.4. Постоянный контроль осуществляется ответственным за организацию обработки персональных данных в Госпитале, администратором ИСПДн Госпиталя с привлечением работников структурных подразделений с целью анализа состояния системы защиты информации и выявления слабых мест в ее организации.

2.1.1.5. Внеплановый контроль проводится при любых изменениях в составе и структуре системы защиты информации, а также условий эксплуатации объектов информационных систем.

2.1.2. По составу проверочной комиссии контроль подразделяется на виды:

– внешний контроль, проводимый ФСБ России, ФСТЭК России и Роскомнадзором;

– внутренний контроль.

2.1.2.1. Внешний контроль осуществляется в соответствии с действующим законодательством и нормативными правовыми актами Российской Федерации и в порядке, установленным контрольным органом.

2.1.2.2. Внутренний контроль проводится:

– ответственным за организацию обработки персональных данных в Госпитале, администратором ИСПДн Госпиталя.

2.1.2.3. По периодичности проведения внутренний контроль подразделяется на:

– периодический;

– повседневный (ежедневный, еженедельный).

2.1.2.4. Мероприятия, проводимые в ходе периодического контроля, должны быть учтены в плане организационных и технических мероприятий по защите информации, в разрезе периодичности проведения контрольных мероприятий (ежегодные, полугодовые, ежеквартальные).

2.1.2.5. Ежегодный внутренний контроль системы защиты информации на объектах информационных технологий Госпиталя проводится с привлечением специализированной организацией, имеющей действующие лицензии на соответствующие виды деятельности.

2.1.2.6. Аттестация объекта информационных технологий по требованиям безопасности информации является одним из видов периодического контроля системы защиты информации на данном объекте.

2.1.2.7. К полугодовым и ежеквартальным проверкам могут быть отнесены проверка знаний работников структурных подразделений Госпиталя требований по

защите информации, мониторинг нормативной правовой базы Российской Федерации в области защиты информации для своевременного внесения изменений во внутренние распорядительные документы и иные мероприятия.

2.1.2.8. Повседневный контроль заключается проверке работоспособности ОТСС, ВТСС и средств защиты информации, актуализации документации на объекты информационных технологий (при необходимости), контролю соблюдения работниками Госпиталя установленных требований по защите информации. Данный контроль проводится в целях оценки состояния наиболее уязвимых элементов системы защиты объектов информационных технологий и своевременного принятия мер по нейтрализации каналов утечки информации.

2.1.2.9. Контроль устранения недостатков, выявленных в ходе ежегодного внутреннего контроля, заключается в проверке устранения выявленных ранее недостатков.

2.2. Итоговое состояние системы защиты информации определяется по совокупности результатов внешнего, внутреннего контроля и по соотношению выявленных и устраненных нарушений требований по защите информации.

3. Объекты, подлежащие контролю и его периодичность

3.1. Объектами контроля в Госпитале являются система защиты информации, эксплуатируемые объекты информационных технологий и их система защиты.

3.2. Объекты проверки при внешнем контроле определяются контролирующими органами.

3.3. Объекты проверки внутреннего контроля в Госпитале:

– структура системы организационных мероприятий по защите информации (комплекс организационных распорядительных документов), их соответствие установленным требованиям в области защиты информации и проверка соблюдения требований по защите информации ответственными лицами и исполнителями (контроль проводится экспертно-документальным методом);

– объекты информационных технологий (контроль проводится экспертно-документальным и инструментальным методами).

3.4. Объект информационных технологий включает в себя:

а) основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи информации ограниченного доступа. В контексте настоящей Инструкции к ОТСС относятся:

– средства вычислительной техники (например: автоматизированное рабочее место в составе: системный блок (терминал), монитор, клавиатура, манипулятор-мышь, источник бесперебойного питания, локальный принтер; серверное оборудование (физическое, виртуальное); системы хранения данных; телекоммуникационное оборудование, средства и системы связи и передачи данных и т.п.);

– средства звуко - видеовоспроизведения (телевизоры, проекторы, системы аудиовоспроизведения и т.п.).

б) вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения информации ограниченного доступа, размещаемые совместно с ОТСС или в защищаемых помещениях. К ВТСС относятся:

– телефонные средства и системы;

– средства и системы передачи данных, системы радиосвязи;

– средства и системы охранной и пожарной сигнализации;

– средства и системы оповещения и сигнализации;

– контрольно-измерительная аппаратура;

– средства и системы кондиционирования;

– средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.п.);

– средства электронной оргтехники;

– иные технические средства и системы.

в) программные и программно-аппаратные средства и системы защиты информации. К таковым, в частности, могут относиться:

– средства защиты информации от несанкционированного доступа;

– средства идентификации и аутентификации (электронные замки, средства авторизации по биометрическим данным, смарт-карты, токены, идентификаторы iButton и т.д.);

– средства криптографической защиты информации, в том числе средства электронной подписи;

– межсетевые экраны;

– системы обнаружения/предотвращения вторжений (IDS/IPS);

– сканеры безопасности;

– средства антивирусной защиты;

– системы предотвращения утечек информации (DLP);

– средства защиты информации от акустической разведки;

– средства защиты информации от утечки по техническим каналам;

– средства гарантированного уничтожения информации на магнитных носителях.

г) системы электропитания, технологического заземления, кондиционирования;

д) системы охраны и сохранности средств, обрабатывающих, передающих и хранящих защищаемую информацию;

– системы пропускного и объектового режима;

– системы видеонаблюдения;

– системы контроля управления доступа;

– системы физической охраны объекта.

е) помещения со средствами (системами) информационных технологий, подлежащими защите.

4. Организация проведения контроля состояния защиты информации

4.1. Организация проведения контроля состояния защиты информации в Госпитале.

4.1.1. Контроль состояния защиты информации в Госпитале проводится ежегодно на основании плана, утверждаемого Главным врачом.

4.1.2. План проверок должен включать наименование мероприятия, периодичность проведения мероприятия и ответственных исполнителей. Типовая форма плана:

Мероприятие	Периодичность	Исполнитель/ Ответственный

4.1.3. План проверок должен включать мероприятия по контролю выполнения требований:

– законодательства и нормативных правовых актов Российской Федерации в области защиты информации;

– внутренних организационных распорядительных документов в области защиты информации, установленных в Госпитале.

4.1.4. В случае обнаружения недостатков разрабатываются рекомендации по их устранению.

4.1.5. Контроль устранения недостатков проводится в ходе следующей проверки состояния защиты информации.

4.1.6. Если для контроля выполнения технических мер по защите информации необходимо привлечение специализированной организации, имеющей действующие лицензии ФСТЭК России и (или) ФСБ России (организация-лицензиат), то привлечение организации-лицензиата для проведения контрольных технических мероприятий производится в установленном законодательством Российской Федерации порядке.

4.2. Организация проведения внутреннего (внутриобъектового) контроля (в т.ч.пропускного режима и порядка охраны).

4.2.1. В ходе контроля проверке подлежит выполнение следующих видов работ:

– оценка актуальности и полноты организационной распорядительной документации в Госпитале (положения, регламенты, инструкции и т.п.);

– проверка наличия эксплуатационной и организационно-распорядительной документации на созданные системы защиты объектов информационных технологий;

– выявление изменений, которые произошли на объектах информационных технологий после предыдущего контроля, и оценка актуальности эксплуатационной и организационно-распорядительной документации на созданные системы защиты в связи с такими изменениями;

– проверка выполнения основных организационных мер по поддержке функционирования средств защиты информации (включение к началу обработки защищаемой информации или оглашения такой информации на соответствующих объектах информационных технологий средств зашумления, проведение технического обслуживания средств защиты информации и т.п.);

– проверка иных требований эксплуатационной и организационно-распорядительной документации на созданные системы защиты объектов информационных технологий.

5. Порядок проведения разбирательств по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности информационных систем, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений

5.1. Инцидент ИБ – одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большой шанс скомпрометировать деловые операции и поставить под угрозу защиту информации (ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности).

5.2. Разбирательство по всем инцидентам ИБ проводится ответственным за организацию обработки персональных данных в Госпитале, администратором ИСПДн Госпиталя.

5.3. Основными источниками информации об инцидентах ИБ являются:

– факты, выявленные руководителем структурного подразделения Госпиталя, ответственным за организацию обработки персональных данных в Госпитале, администратором ИСПДн Госпиталя, а также другими работниками Госпиталя.

– результаты работы средств мониторинга (журналы событий средств защиты информации);

– результаты контроля (внутреннего или внешнего);

– обращения субъектов персональных данных с указанием инцидента ИБ;

– запросы и предписания уполномоченных органов (ФСБ России, ФСТЭК России, Роскомнадзор, органы прокуратуры);

– другие источники информации.

5.4. Работник Госпиталя может выявить признаки наличия инцидента ИБ путем анализа текущей ситуации на предмет ее соответствия утвержденных в Госпитале

требований. Выявленные несоответствий дают основания предполагать факт возникновения инцидента ИБ. Любые сведения об инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником ответственному за организацию обработки персональных данных в Госпитале, администратору ИСПДн Госпиталя.

5.5. Ответственный за организацию обработки персональных данных в Госпитале, администратор ИСПДн Госпиталя после получения информации о предполагаемом (совершенном) инциденте ИБ незамедлительно проводят первоначальный анализ полученных данных. В процессе анализа проводится проверка наличия в выявленном факте нарушений.

5.6. В случае нарушения прав субъекта персональных данных разбирательство и реагирование происходит в порядке и сроки, предусмотренные установленными в Госпитале «Правилами рассмотрения запросов субъектов персональных данных, или их представителей в государственном бюджетном учреждении Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн».

5.7. В случае наличия признаков инцидента ИБ в полученной информации, ответственным за организацию обработки персональных данных в Госпитале, администратором ИСПДн Госпиталя определяется предварительную степень важности инцидента ИБ и принимается решение о необходимости проведения разбирательства.

5.8. Разбирательство инцидента ИБ, в общем, состоит из следующих этапов:

– подтверждение/опровержение факта возникновения инцидента ИБ;

– подтверждение/корректировка уровня значимости инцидента ИБ;

– уточнение дополнительных обстоятельств (деталей) инцидента ИБ;

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

– минимизация последствий инцидента ИБ;

– информирование и консультирование работников Госпиталя по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;

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

5.9. При обнаружении уязвимостей или факта НСД незамедлительно проводятся меры, направленные на локализацию инцидента и на минимизацию его последствий. Для проведения разбирательства создается комиссия, состав которой утверждается Главным врачом. В состав комиссии в обязательном порядке включаются ответственный за организацию обработки персональных данных в Госпитале, администратор ИСПДн Госпиталя, работник, обнаруживший факт НСД, руководители и работники других структурных подразделений Госпиталя в зависимости от характера технологических процессов и ресурсов, затронутых инцидентом ИБ, приведшем к НСД. Взаимодействие между членами комиссии осуществляется в рабочем порядке с соблюдением при этом требований конфиденциальности. При необходимости проводятся заседания комиссии, время, место и темы которых определяются ее председателем.

5.10. В процессе проведения разбирательства инцидента ИБ обязательными для установления являются:

– дата и время совершения инцидента ИБ;

– Ф.И.О, должность и подразделение нарушителя (работника, допустившего факт НСД);

– уровень критичности инцидента ИБ;

– обстоятельства, способствовавшие совершению инцидента ИБ;

– мотивы совершения инцидента ИБ;

– информационные ресурсы, затронутые инцидента ИБ;

– характер и размер реального и потенциального ущерба.

5.11. При необходимости в ходе проведения разбирательства может быть запрошена информация в структурных подразделениях Госпиталя. Запрос направляется на имя руководителя структурного подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки). В случае получения объяснительных, ответ должен быть представлен в течение 3 (трех)

рабочих дней с момента поступления запроса. В случае отказа предоставить объяснительную записку, данный факт отражается в материалах разбирательства.

5.12. Результат работы разбирательства оформляется актом. Собранные в процессе разбирательства материалы прикладываются к акту.

5.13. По завершению разбирательства инцидента ИБ, совершенного работником Госпиталя, материалы разбирательства (в объеме, достаточном для принятия решения) передаются Главному врачу для решения вопроса о целесообразности привлечения нарушителя к дисциплинарной ответственности.

5.14. На основании полученных результатов Главный врач организовывает проведение мероприятий, направленных на снижение рисков ИБ в будущем:

– анализ и пересмотр имеющихся прав доступа к информационным ресурсам Госпиталя у данного работника;

– доведение до всех работников требований по защите информации;

– отмена неактуальных прав доступа к информационным ресурсам;

– пересмотр частных моделей угроз безопасности информации и моделей нарушителя;

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к информации и (или) ее передачи лицам, не имеющим права доступа к ней.

– другие обоснованные мероприятия.

5.15. Работники Госпиталя, осуществляющие разбирательство имеют право:

– по согласованию с непосредственным руководителем работника, действия которого привели к инциденту ИБ, требовать предоставлений письменных объяснений по обстоятельствам инцидента ИБ у этого работника;

– запрашивать и получать от руководителей структурных подразделений и работников Госпиталя, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства Инцидента ИБ.

– инициировать блокировку учетных записей (или отключение прав доступа к информационным ресурсам) работников Госпиталя, нарушивших требования по защите информации, на период проведений расследования инцидента ИБ в случае, если имеется существенный риск того, что продолжение их работы может повлечь значительное увеличение ущерба или новые инциденты ИБ.

– по результатам расследования инцидента ИБ инициировать изменения в технологических процессах и информационных ресурсах Госпиталя с целью повышения их защищенности и снижения рисков инцидентов ИБ.

– инициировать процедуры привлечения нарушителей к дисциплинарной/материальной ответственности.

5.16. Работники Госпиталя, осуществляющие разбирательств обязаны:

– объективно и основательно проводить разбирательство каждого инцидента ИБ.

– определять все необходимые меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий.

– фиксировать всю информацию, полученную в ходе разбирательства, и вести учет инцидентов ИБ;

– предоставлять Главному врачу отчеты и рекомендации по проведенным разбирательствам;

– проводить анализ обстоятельств, способствовавших совершению каждого инцидента ИБ, и на его основе, совместно с работниками смежных структурных подразделений, разрабатывать рекомендации и предложения по оптимизации технологических процессов и снижения ущерба от подобных инцидентов ИБ и минимизации возможности их повторения в будущем.

Приложение 1
к Инструкции по контролю эффективности
состояния системы защиты информации в
государственном бюджетном учреждении
Рязанской области «Рязанский областной
клинический госпиталь для ветеранов войн»

Методика
формирования плана организационных и технических мероприятий по защите информации и перечень включаемых в него рекомендуемых мероприятий

1. План организационных и технических мероприятий по защите информации (План) определяет перечень предполагаемых к проведению мероприятий по защите информации, сроки их выполнения, ответственных исполнителей, и предназначен для эффективного управления и контроля за системой защиты информации в Госпитале.

2. План формируется ежегодно в конце календарного года и утверждается Главным врачом.

3. Все ответственные исполнители, задействованные в проведении мероприятий, указанных в Плане, должны быть ознакомлены с ним под роспись.

4. При необходимости могут быть разработаны полугодовые, ежеквартальные планы.

5. Планирование работ по защите информации осуществляется по следующим основным направлениям:

– обеспечение эффективного управления системой защиты информации. Основными мероприятиями в области обеспечения эффективного управления системой защиты информации в Госпитале являются:

– регулярный мониторинг действующего законодательства Российской Федерации в области защиты информации;

– разработка, регулярная актуализация в целях соответствия действующему законодательству Российской Федерации внутренней организационной распорядительной документации в области защиты информации и ознакомление с ней работников Госпиталя;

– ознакомление работников Госпиталя с требованиями по защите информации, их обучение правилам использования средств защиты информации;

– повышение квалификации ответственных за обеспечение безопасности информации (работников, отвечающих за безопасность информации на объектах информационных технологий) на специализированных курсах, согласованных в ФСТЭК России (Постановление Правительства РФ от 6 мая 2016 г. № 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса»);

– определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения. Например, к таким мероприятиям относится ежегодный пересмотр перечня сведений конфиденциальной информации (информации ограниченного доступа) в Госпитале.

– анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки информации, подлежащих защите. К таким мероприятиям могут относится:

– комплексный анализ инцидентов ИБ;

– моделирование угроз безопасности информации и нарушителя при разработке объектов информационных технологий, и пересмотр моделей с учетом развития

информационных технологий и анализа инцидентов ИБ, произошедших, как непосредственно в Госпитале, так и в других учреждениях и организациях;

– разработка и реализация мер, необходимых для устранения актуальных угроз безопасности информации;

– иные мероприятия.

– разработка организационно-технических мероприятий по защите информации и их реализация.

Основными организационно-техническими мероприятиями по защите информации в Госпитале являются:

– разработка и реализация разрешительной системы доступа на объектах информационных технологий;

– аттестация объектов по выполнению требований обеспечения защиты информации (автоматизированные системы, защищаемые помещения, информационные системы персональных данных, государственные информационные системы (в т.ч. информационные системы общего пользования, ключевые системы информационных инфраструктур;

– обеспечение условий защиты информации при подготовке и реализации договорных отношений;

– создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

– применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

– организация и проведение контроля состояния защиты информации. В данном направлении учитываются как мероприятия, проводимые в ходе внутреннего и внутриобъектового контроля, так и мероприятия по подготовке к внешнему контролю.

6. Конкретные методы, приемы и меры защиты информации разрабатываются в зависимости от степени возможного ущерба в случае ее утечки, разрушения (уничтожения).

7. Проведение любых мероприятий и работ с использованием информации, обрабатываемой на объектах информационных технологий и обсуждаемых в защищаемых помещениях, без принятия необходимых мер по защите информации не допускается.

Приложение № 28
к приказу ГБУ РО РОКГВВ
от «09» января 2020 г. № 47

РУКОВОДСТВО

пользователя информационных систем государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее руководство определяет права и обязанности Пользователя информационных систем государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн» (далее – пользователь ИС).

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

2.1. Пользователи ИС обязаны знать и выполнять требования законодательства РФ, приказов главного врача государственного бюджетного учреждения Рязанской области «Рязанский областной клинический госпиталь для ветеранов войн», устанавливающих правила обработки и защиты информации в ИС, в том числе персональных данных (далее – ПДн).

2.2. При эксплуатации ИС с целью защиты информации, в том числе ПДн, пользователь ИС обязан:

– руководствоваться требованиями организационно – распорядительной документации по организации обработки и защиты информации в ИС;

– соблюдать установленную технологию обработки и защиты информации;

– использовать для записи информации ИС только съемные носители информации, учтенные в установленном порядке;

– использовать для вывода на печать документов, содержащих информацию, находящуюся в ИС, только устройства печати, расположенные в пределах установленных контролируемых зон, сводя к минимуму возможность доступа к ним посторонних лиц.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам вычислительной техники (далее – СВТ) ИС посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на СВТ работ. В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются СВТ ИС, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить СВТ. Защищаемые носители информации должны быть убраны в запираемые хранилища, определенные в установленном порядке для этих целей.

2.4. Пользователь обязан докладывать ответственному за организацию обработки персональных данных в Госпитале, администратору ИСПДн Госпиталя и своему непосредственному руководителю:

– о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, СВТ ИС, помещениям, в которых располагаются СВТ ИС, и хранилищам;

– об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка информации ИС и хранилищ;

– об обнаружении вредоносного программного обеспечения или нетипичного поведения ИС;

– о попытках получения информации лицами, не имеющими к ней допуска;

– об иных внештатных ситуациях, связанных с угрозой безопасности ИС;

2.5. Пользователю запрещается:

– подключать к СВТ ИС нештатные устройства;

– самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку

программного обеспечения, установленного в ИС;

– самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) ИС;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к ИС;

– разрешать работу с СВТ ИС лицам, не допущенным в установленном порядке к обработке информации в ИС.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ ИС

3.1. Пользователь ИС имеет право:

– обращаться к администратору ИСПДн Госпиталя по любым вопросам, касающихся обработки и защиты информации в ИС (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации ИС);

– обращаться к администратору ИСПДн Госпиталя с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в ИС информации, а также по вопросам эксплуатации установленных средств защиты информации (СЗИ);

– обращаться к администратору ИСПДн Госпиталя с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств ИС.

4. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС

4.1. Пользователь ИС несет ответственность:

– за соблюдение установленной технологии обработки информации в ИС, в том числе ПДн;

– за соблюдение режима конфиденциальности информации;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИС;

– за соблюдение требований локальных актов по вопросам обработки и защиты информации в ИС, в том числе ПДн.

4.2. Пользователи ИС, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Руководством, в пределах, определенных действующим законодательством Российской Федерации.