Приложение № 3 к приказу

от 02 09 2019 г. № 31

Государственное бюджетное учреждение здравоохранения

Ярославской области "Рыбинская городская больница № 1"

**Политика**

информационной безопасности

информационных систем персональных данных

**г. Рыбинск**

**2019**

#

# Введение

Настоящая Политика информационной безопасности государственного бюджетного учреждения здравоохранения Ярославской области "Рыбинская городская больница № 1 (далее ГБУЗ ЯО "Рыбинская городская больница № 1") разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПД ГБУЗ ЯО "Рыбинская городская больница № 1".

Политика разработана в соответствии с требованиями нормативных документов, указанных в приложении № 1 "Определения и сокращения. Список нормативных документов" к настоящему приказу.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн ГБУЗ ЯО "Рыбинская городская больница № 1".

# Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты ГБУЗ ЯО "Рыбинская городская больница № 1" от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

Состав ИСПДн подлежащих защите, представлен в Отчете о результатах проведения внутренней проверки.

# Область действия

Требования настоящей Политики распространяются на всех сотрудников ГБУЗ ЯО "Рыбинская городская больница № 1" (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

# 1. Система защиты персональных данных

1.1. Система защиты персональных данных (СЗПДн), строится на основании:

* Отчета о результатах проведения внутренней проверки;
* Перечня персональных данных, подлежащих защите;
* Определения уровня защиты ИСПДн;
* Модели угроз безопасности персональных данных;
* Положения о разграничении прав доступа к обрабатываемым персональным данным;
* Руководящих и методических документов Минздрава РФ, ФСТЭК и ФСБ России.

1.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн ГБУЗ ЯО "Рыбинская городская больница № 1". На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверке, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

1.3. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

* АРМ пользователей;
* Сервера приложений;
* СУБД;
* Граница ЛВС;
* Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

1.4. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

* антивирусные средства для рабочих станций пользователей и серверов;
* средства межсетевого экранирования;
* средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

1.5. Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

* управление и разграничение доступа пользователей;
* регистрацию и учет действий с информацией;
* обеспечивать целостность данных;
* производить обнаружений вторжений.

1.6. Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем ГБУЗ ЯО "Рыбинская городская больница № 1" или лицом, ответственным за обеспечение защиты ПДн.

# 2. Требования к подсистемам СЗПДн

 СЗПДн включает в себя следующие подсистемы:

* управления доступом, регистрации и учета;
* обеспечения целостности и доступности;
* антивирусной защиты;
* межсетевого экранирования;
* анализа защищенности;
* обнаружения вторжений;
* криптографической защиты.

 Подсистемы СЗПДн имеют различный функционал в зависимости от требуемого уровня защиты ИСПДн.

## 2.1. Подсистемы управления доступом, регистрации и учета

2.1.1. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

* идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
* идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
* идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
* регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
* регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
* регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

2.1.2. Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

## 2.2. Подсистема обеспечения целостности и доступности

2.2.1. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн ГБУЗ ЯО "Рыбинская городская больница № 1", а также средств защиты, при случайной или намеренной модификации.

2.2.2. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

## 2.3. Подсистема антивирусной защиты

2.3.1. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн ГБУЗ ЯО "Рыбинская городская больница № 1".

2.3.2. Средства антивирусной защиты предназначены для реализации следующих функций:

* резидентный антивирусный мониторинг;
* антивирусное сканирование;
* скрипт-блокирование;
* централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
* автоматизированное обновление антивирусных баз;
* ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
* автоматический запуск сразу после загрузки операционной системы.

2.3.3. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

## 2.4. Подсистема межсетевого экранирования

2.4.1. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

* фильтрации открытого и зашифрованного (закрытого) IP-трафика;
* фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
* идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;
* регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
* контроля целостности своей программной и информационной части;
* фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
* регистрации и учета запрашиваемых сервисов прикладного уровня;
* блокирования доступа не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
* контроля за сетевой активностью приложений и обнаружения сетевых атак.

2.4.2. Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ.

## 2.5. Подсистема анализа защищенности

2.5.1. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

2.5.2. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

## 2.6. Подсистема обнаружения вторжений

2.6.1. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

2.6.2. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

## 2.7. Подсистема криптографической защиты

2.7.1. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн ГБУЗ ЯО "Рыбинская городская больница № 1", при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

2.7.2. Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

# 3. Пользователи ИСПДн

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн ГБУЗ ЯО "Рыбинская городская больница № 1" можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

* Администратора ИСПДн;
* Администратора безопасности;
* Оператора АРМ;
* Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.

## 3.1. Администратор ИСПДн

3.1.1. Администратор ИСПДн, сотрудник ГБУЗ ЯО "Рыбинская городская больница № 1", ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

3.1.2. Администратор ИСПДн обладает следующим уровнем доступа и знаний:

* обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
* обладает полной информацией о технических средствах и конфигурации ИСПДн;
* имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
* обладает правами конфигурирования и административной настройки технических средств ИСПДн.

## 3.2. Администратор безопасности

3.2.1. Администратор безопасности, сотрудник ГБУЗ ЯО "Рыбинская городская больница № 1", ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

3.2.2. Администратор безопасности обладает следующим уровнем доступа и знаний:

* обладает правами Администратора ИСПДн;
* обладает полной информацией об ИСПДн;
* имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
* не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).
* Администратор безопасности уполномочен:
* реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
* осуществлять аудит средств защиты;
* устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

## 3.3. Оператор АРМ

3.3.1. Оператор АРМ, сотрудник ГБУЗ ЯО "Рыбинская городская больница № 1", осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

3.3.2. Оператор ИСПДн обладает следующим уровнем доступа и знаний:

* обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
* располагает конфиденциальными данными, к которым имеет доступ.

## 3.4. Программист-разработчик ИСПДн

3.4.1. Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники ГБУЗ ЯО "Рыбинская городская больница № 1", так и сотрудники сторонних организаций.

3.4.2. Лицо этой категории:

* обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
* обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
* может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

# 4. Требования к персоналу по обеспечению защиты ПДн

4.1. Все сотрудники ГБУЗ ЯО "Рыбинская городская больница № 1", являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

4.2. При вступлении в должность нового сотрудника непосредственный руководитель подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

4.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

4.4. Сотрудники ГБУЗ ЯО "Рыбинская городская больница № 1", использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

4.5. Сотрудники ГБУЗ ЯО "Рыбинская городская больница № 1" должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

4.6. Сотрудники ГБУЗ ЯО "Рыбинская городская больница № 1" должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

4.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

4.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ГБУЗ ЯО "Рыбинская городская больница № 1", третьим лицам.

4.9. При работе с ПДн в ИСПДн сотрудники ГБУЗ ЯО "Рыбинская городская больница № 1" обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

4.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

4.11. Сотрудники ГБУЗ ЯО "Рыбинская городская больница № 1" должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

4.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

# 5. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

* Инструкция администратора ИСПДн;
* Инструкция администратора безопасности ИСПДн;
* Инструкция пользователя ИСПДн;
* Инструкция пользователя при возникновении внештатных ситуаций.

# 6. Ответственность сотрудников ИСПДн ГБУЗ ЯО "Рыбинская городская больница № 1"

6.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

6.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации, распространению информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

6.3. При нарушениях сотрудниками ГБУЗ ЯО "Рыбинская городская больница № 1" – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

6.4. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях ГБУЗ ЯО "Рыбинская городская больница № 1", осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников ГБУЗ ЯО "Рыбинская городская больница № 1".

6.5. Необходимо внести в Положения о подразделениях ГБУЗ ЯО "Рыбинская городская больница № 1", осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.