

ФБУ «Белгородский ЦСМ»	Система менеджмента качества Положение о порядке организации работ с персональными данными и обеспечению их безопасности при обработке в информационной системе персональных данных ФБУ «Белгородский ЦСМ»	Лист 32 Листов 143
	И-СМК-005-2018	

Приложение 2

Политика безопасности персональных данных в информационной системе персональных данных ФБУ «Белгородский ЦСМ»

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее - Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных в информационной системе персональных данных ФБУ «Белгородский ЦСМ».

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В Политике определены требования к персоналу ФБУ «Белгородский ЦСМ», степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ФБУ «Белгородский ЦСМ».

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Целью настоящей Политики является обеспечение безопасности объектов защиты ФБУ «Белгородский ЦСМ» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.

1.2 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.

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

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

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

ФБУ «Белгородский ЦСМ»	Система менеджмента качества Положение о порядке организации работ с персональными данными и обеспечению их безопасности при обработке в информационной системе персональных данных ФБУ «Белгородский ЦСМ»	Лист 33 Листов 143
	И-СМК-005-2018	

2 ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящей Политики распространяются на всех сотрудников ФБУ «Белгородский ЦСМ» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

- отчета о результатах проведения внутренней проверки;
- перечня персональных данных, подлежащих защите;
- акта классификации информационной системы персональных данных;
- модели угроз безопасности персональных данных;
- положения о разграничении прав доступа к обрабатываемым персональным данным;
- руководящих документов ФСТЭК и ФСБ России.

3.2 На основании этих документов определяется необходимый уровень защищенности ПДн в ФБУ «Белгородский ЦСМ». На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, и Акта о результатах проведения проверки 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.

3.3 Для каждого сегмента ИСПДн ФБУ «Белгородский ЦСМ» должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- серверы приложений;
- СУБД;
- граница ЛВС;
- каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

3.4 В зависимости от установленного уровня защищенности ИСПДн ФБУ «Белгородский ЦСМ» и актуальных угроз СЗПДн может включать следующие технические средства:

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

3.5 Также в список включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и

ФБУ «Белгородский ЦСМ»	Система менеджмента качества Положение о порядке организации работ с персональными данными и обеспечению их безопасности при обработке в информационной системе персональных данных ФБУ «Белгородский ЦСМ»	Лист 34 Листов 143
	И-СМК-005-2018	

специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

3.6 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 ФБУ «Белгородский ЦСМ» соответствующие изменения должны быть внесены в Список и утверждены директором ФБУ «Белгородский ЦСМ» или лицом, ответственным за обеспечение защиты ПДн.

4 ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДн

4.1 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.

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

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн ФБУ «Белгородский ЦСМ»;
- 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 остановка;
- 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.

4.3 Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн ФБУ «Белгородский ЦСМ», а также средств защиты при случайной или намеренной модификации.

ФБУ «Белгородский ЦСМ»	Система менеджмента качества Положение о порядке организации работ с персональными данными и обеспечению их безопасности при обработке в информационной системе персональных данных ФБУ «Белгородский ЦСМ»	Лист 35 Листов 143
	И-СМК-005-2018	

4.4 Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн ФБУ «Белгородский ЦСМ».

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.

4.5 Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по определенным параметрам;
- 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;
- 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 неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

4.6 Подсистема анализа защищенности должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн ФБУ «Белгородский ЦСМ», которые могут быть использованы нарушителем для реализации атаки на систему.

4.7 Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы ИСПДн ФБУ «Белгородский ЦСМ», подключенные к сетям общего пользования и (или) международного обмена.

ФБУ «Белгородский ЦСМ»	Система менеджмента качества	Лист 36 Листов 143
	Положение о порядке организации работ с персональными данными и обеспечению их безопасности при обработке в информационной системе персональных данных ФБУ «Белгородский ЦСМ»	
И-СМК-005-2018		

4.8 Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации ИСПДн ФБУ «Белгородский ЦСМ» при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

5 ПОЛЬЗОВАТЕЛИ ИСПДН ФБУ «БЕЛГОРОДСКИЙ ЦСМ»

5.1 В ИСПДн ФБУ «Белгородский ЦСМ» выделяются следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор безопасности ИСПДн ФБУ «Белгородский ЦСМ»;
- администратор системный ИСПДн;
- оператор АРМ.

5.2 Данные о группах пользователей, уровне их доступа и информированности отражен в Положении о разграничении прав доступа к обрабатываемым персональным данным.

6 ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

6.1 Все сотрудники ФБУ «Белгородский ЦСМ», являющиеся пользователями ИСПДн ФБУ «Белгородский ЦСМ», должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

6.2 При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн ФБУ «Белгородский ЦСМ».

6.3 Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн ФБУ «Белгородский ЦСМ» и СЗПДн.

6.4 Сотрудники ИСПДн ФБУ «Белгородский ЦСМ», 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.

6.5 Сотрудники ИСПДн ФБУ «Белгородский ЦСМ» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

6.6 Сотрудники ИСПДн ФБУ «Белгородский ЦСМ» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи

ФБУ «Белгородский ЦСМ»	Система менеджмента качества Положение о порядке организации работ с персональными данными и обеспечению их безопасности при обработке в информационной системе персональных данных ФБУ «Белгородский ЦСМ»	Лист 37 Листов 143
	И-СМК-005-2018	

должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

6.7 Сотрудникам ИСПДн ФБУ «Белгородский ЦСМ» запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

6.8 Сотрудникам ИСПДн ФБУ «Белгородский ЦСМ» запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.

6.9 При работе с ПДн в ИСПДн ФБУ «Белгородский ЦСМ» сотрудники обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

6.10 При завершении работы с ИСПДн ФБУ «Белгородский ЦСМ» сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентным средством контроля, например, доступом по паролю, если не используются более сильные средства защиты.

6.11 Сотрудники ФБУ «Белгородский ЦСМ» 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.

6.12 Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн ФБУ «Белгородский ЦСМ», 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.

7 ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИСПДН ФБУ «БЕЛГОРОДСКИЙ ЦСМ»

Обязанности пользователей ИСПДн описаны в следующих документах:

- руководство администратора системного информационной системы персональных данных ФБУ «Белгородский ЦСМ»;
- руководство администратора безопасности при использовании ресурсов объекта вычислительной техники – информационной системы персональных данных ФБУ «Белгородский ЦСМ»;
- руководство пользователю информационной системы персональных данных ФБУ «Белгородский ЦСМ».

ФБУ «Белгородский ЦСМ»	Система менеджмента качества Положение о порядке организации работ с персональными данными и обеспечению их безопасности при обработке в информационной системе персональных данных ФБУ «Белгородский ЦСМ»	Лист 38 Листов 143
	И-СМК-005-2018	

8 ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ ИСПДН ФБУ «БЕЛГОРОДСКИЙ ЦСМ»

8.1 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 информации или нарушению работы ЭВМ или сетей (ст.ст. 272 - 274 Уголовного кодекса РФ).

8.2 Администратор системный ИСПДн ФБУ «Белгородский ЦСМ» и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

8.3 При нарушениях сотрудниками - пользователями ИСПДн ФБУ «Белгородский ЦСМ» правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

8.4 Приведенные выше требования нормативных документов по защите информации должны быть отражены в руководствах сотрудников ИСПДн ФБУ «Белгородский ЦСМ».