Приложение № 1
к приказу от17.05.2018 г № 85-од

Политика
информационной безопасности в области обработки и защиты персональных данных муниципального бюджетного учреждения культуры «Мончегорская централизованная библиотечная система» (МБУ ЦБС)

1.Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о ПДн) и является основополагающим внутренним регламентирующим документом муниципального бюджетного учреждения культуры «Мончегорская централизованная библиотечная система» (далее – МБУ ЦБС), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является МБУ ЦБС.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод гражданина при обработке его ПДн в МБУ ЦБС.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных МБУ ЦБС как до, так и после утверждения Политики.

1.4. В Политике определены требования к работникам МБУ ЦБС работающим с ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности ИСПДн, должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в ИСПДн МБУ ЦБС.

1.5**.** Основные понятия и сокращения используемые в настоящей Политике:

- **персональные данные(ПДн)** - любая информация, относящаяся к определенному физическому лицу (пользователю библиотеки), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- **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;
- **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;
- **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;
- **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;
- **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной

системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;
- **информационная система персональных данных** (ИСПДн) - 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 или без использования таких средств;
- автоматизированное рабочее место (АРМ)
- **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Область действия

2.1. Требования настоящей Политики распространяются на всех работников МБУ ЦБС (штатных, временных, работающих по договору и т.п.)

3. Система защиты персональных данных

3.1. Система защиты персональных данных (далее- СЗПДн) включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3.2 Выбор средств защиты информации для системы защиты персональных данных осуществляется МБУ ЦБС в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона "О персональных данных".

3.3. Система защиты персональных данных (СЗПДн), строится на основании:
- отчёта о результатах обследования МБУ ЦБС в части требований законодательства РФ по вопросам обеспечения информационной безопасности в ИСПДн;
- акта классификации информационной системы персональных данных;
- инструкции по обработке персональных данных пользователей МБУ ЦБС;
- инструкции по обработке персональных данных работников МБУ ЦБС;
- частной модели угроз безопасности персональных данных при их обработке в ИСПДн «ИРБИС. Центр регистрации читателей»;
- частной модели угроз безопасности персональных данных при их обработке в ИСПДн «1С Предприятие. 8.3 Зарплата + Кадры»;
- руководящих документов ФСТЭК и ФСБ России.

3.4. На основании документов, указанных в п. 3.3 определяется необходимый уровень защищённости ПДн каждой ИСПДн МБУ ЦБС.

3.5. На основании анализа актуальных угроз безопасности ПДн описанного в Моделях угроз делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Мероприятия отражаются в «Плане мероприятий по обеспечению защиты ПДн».

3.6. Для ИСПДн МБУ ЦБС определены используемые технические средств защиты, а так же программное обеспечение, участвующее в обработке ПДн. Средства защиты ПДн включают:

- системы управления и разграничения прав доступа;
- штатные средства обработки ПДн операционными системами (ОС),
- прикладным ПО: антивирус Касперского, «КриптоПро CSP», Dallas Lock 7.7;
- установка индивидуальных паролей для доступа к программному обеспечению ИСПДн (ИРБИС 64) лицам, имеющими право доступа к ПДн.

3.7. Функции защиты обеспечивают целостность данных и позволяют производить обнаружение вторжений.

3.8.Список используемых технических средств отражается в «Плане мероприятий по обеспечению защиты персональных данных в МБУ ЦБС». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список лицом, ответственным за обеспечение защиты ПДн.

3.9 Требования к подсистемам СЗПДн.

3.9.1 СЗПДн включает в себя следующие подсистемы:

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

3.9.2 Подсистема СЗПДн имеет функционал в зависимости от класса ИСПДн, определенного в «Акте классификации информационной системы персональных данных».

3.10 Подсистемы управления доступом, регистрации и учета.

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

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн по индивидуальным паролям;
- идентификации записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы),
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

Подсистема управления доступом реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД).

3.11 .Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн МБУ ЦБС, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных.

3.12 .Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн МБУ ЦБС.

Средства антивирусной защиты предназначены для реализации следующих функций: 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 изменения настроек антивирусного программного обеспечения; автоматический запуск сразу после загрузки операционной системы,

Подсистема реализуется путем внедрения антивирусного программного обеспечения на все рабочие станции, используемые в МБУ ЦБС.

3.1.3.Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

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

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

3.14. Подсистема анализа защищенности.

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

Функционал подсистемы реализован программными и программно-аппаратными средствами.

3.15. Подсистема обнаружения вторжений.

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования.

Функционал подсистемы реализован программными и программно-аппаратными средствами.

4. Пользователи ИСПДн

4.1. В МБУ ЦБС выделены следующие группы пользователей, участвующих в обработке и хранении ПДн: Администратор ИСПДн, Администратор безопасности ИСПдн; Операторы АРМ, Технический специалист по обслуживанию периферийного оборудования

4.2 Администратор ИСПДн.

Администратор ИСПДн - сотрудник, 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. 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.

4.3 Администратор безопасности.

Администратор безопасности - сотрудник, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент. 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.

4.4. Оператор АРМа.

Оператор АРМа - сотрудник, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование отчетов, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн. Оператор ИСПДн обладает следующим уровнем доступа и знаний: обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к ПДн.

4.5 Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Учреждения, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

5. Требования к персоналу по обеспечению защиты ПДн.

5.1. Все сотрудники МБУ ЦБС, являющиеся операторами ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

5.2. 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 работы с ИСПДн.

5.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, инструкциями по работе с ИСПДн и СЗПДн.

5.4. Сотрудники МБУ ЦБС должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

5.5. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
5.6. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами МБУ ЦБС, третьим лицам.
5.7. При работе с ПДн в ИСПДн сотрудники МБУ ЦБС обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.
5.8. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ, например, доступом по паролю, если не используются более сильные средства защиты.
5.9. Сотрудники МБУ ЦБС должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

6. Ответственность сотрудников, пользователей ИСПДн МБУ ЦБС.

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. Администратор ИСПДн 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.
6.3. При нарушениях сотрудниками МБУ ЦБС – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

7. Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

- Федеральный закон от 27.06.2006 г. № 152-ФЗ «О персональных данных»
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Указ Президента Российской Федерации от 17.03.2008 N 351 О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена (с изменениями на 22 мая 2015 года)
- Постановление Правительства РФ от 21.03.2012 № 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»;
- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК от 14 марта 2014 года N 31 Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих

повышенную опасность для жизни и здоровья людей и для окружающей природной среды (с изменениями на 23 марта 2017 года)

- Приказ Федеральной службы по техническому и экспортному контролю от 05.02.2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»
- Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13.02.2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"
- Приказ Минкомсвязи России от 21.12.2011 № 346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных».
- ГОСТ Р 53113.1-2008 "Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения". М.: Стандартинформ, 2008.
- ГОСТ Р 53113.2-2009 "Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов.
- Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г.
- Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (23.12.2009 г., согласованы с ФСТЭК).
- Методические рекомендации по составлению частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений и организаций здравоохранения, социальной сферы, труда и занятости (23.12.2009 г., согласованы с ФСТЭК).