Утверждено

И.о. директора ГБУК СахОДБ

О. А. Корниенко

приказ № 11 от 31.01.2022 г.

Положение
о порядке организации и проведения работ по защите информации ограниченного распространения (персональных данных) при их обработке в государственном бюджетном учреждении культуры «Сахалинская областная детская библиотека»

1. Общие положения

1.1. Настоящее Положение устанавливает требования к обеспечению безопасности информации (персональных данных) при ее обработке в информационных системах (далее – ИС) государственного бюджетного учреждения культуры «Сахалинская областная детская библиотека» (далее - СахОДБ), представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации и без использования таковых.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими нормативно-правовыми актами, регламентирующими обращение и защиту персональных данных.

2. Порядок определения защищаемых информационных ресурсов

2.1. В соответствии с действующим законодательством, СахОДБ является оператором персональных данных и обрабатывает информационные ресурсы, содержащие персональные данные, в пределах своих полномочий, установленных в соответствии с федеральным и областным законодательством, а также организационно-распорядительными документами СахОДБ (далее – ОРД) в целях обеспечения реализации прав субъектов персональных данных (далее субъектов ПДн).

2.2. В соответствии с ОРД в СахОДБ определяется и утверждается содержание, состав и объем обрабатываемых персональных данных.

2.3. В соответствии с ОРД в СахОДБ определяется и утверждается перечень ИС.

2.4. При проектирования вновь создаваемой или документировании ранее созданной (эксплуатируемой) ИС определяются цели и содержание обработки персональных данных, определяемые действующим законодательством, и утверждается перечень обрабатываемых персональных данных.

3. Основные условия проведения обработки персональных данных в ИС

3.1. Должностные лица СахОДБ, осуществляющие обработку персональных данных в ИС, являются пользователями ИС и обязаны принимать необходимые организационные и технические меры для их защиты.

3.2. Пользователи ИС или иные должностные лица, на законных основаниях получившие доступ к персональным данным, обязаны не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

3.3. Для планирования, разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в ИС распорядительным документом назначаются ответственные должностные лица.

3.4. Должностными лицами СахОДБ, получающими доступ к персональным данным в ИС СахОДБ, должна обеспечиваться конфиденциальность таких данных.

4. Обработка персональных данных в ИС

4.1. Не допускается обработка персональных данных в ИС при отсутствии комплексной системы защиты информации, соответствующей требованиям нормативно-правовых актов и ОРД СахОДБ.

5. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИС

5.1. Допуск к обработке персональных данных ответственных должностных лиц осуществляется на основании утвержденного списка (перечня).

5.2. Должностные лица СахОДБ (далее – пользователи) имеют право в отведенное им рабочим распорядком или распоряжением руководителя структурного подразделения время решать поставленные задачи в соответствии с полномочиями доступа к информационным ресурсам ИС.

5.3. Доступ пользователям к ресурсам ИС осуществляется на основании персональных идентификаторов или паролей.

5.4. Запись и хранение информации, содержащей персональные данные , может осуществляться пользователями только на учтенные в установленном порядке электронные носители информации.

5.5. Пользователи, участвующие в автоматизированной обработке персональных данных и имеющие доступ к аппаратным средствам, программному обеспечению и данным ИС, несут персональную ответственность за свои действия и обязаны:

- соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;
- знать и выполнять правила работы со средствами защиты информации, установленными на автоматизированных рабочих местах (далее - АРМ);
- обеспечивать конфиденциальность персональных паролей и сохранность персональных идентификаторов (ключей);
- выполнять требования по проведению антивирусной защиты в полном объеме.

5.6. Пользователи обязаны извещать руководителя структурного подразделения и ведущего инженера-программиста в случае:

- утери персонального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей;
- обнаружения нарушений целостности пломб (наклеек), нарушении или несоответствии номеров печатей на составляющих узлах и блоках АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД);
- несанкционированных изменений в конфигурации программных или аппаратных средств ИС;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств;
- обнаружения ошибок или сбоев функционирования средств защиты информации;
- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

5.7. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;
- создавать (преднамеренно или непреднамеренно) возможность для ознакомления с защищаемой информацией лиц, не допущенных к персональным данным, в том числе оставлять без личного присмотра на рабочем месте персональный идентификатор, машинные носители и документы, содержащие защищаемую информацию, либо размещать средства отображения информации таким образом, чтобы создавалась возможность визуального просмотра информации;

- записывать и хранить персональные данные и другую конфиденциальную информацию на неучтенных носителях информации;

- оставлять АРМ без присмотра во включенном состоянии, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению предпосылок или угроз утечки (неправомерной модификации) персональных данных.

6. Порядок резервирования информации и восстановления работоспособности технических средств и программного обеспечения ИС, а также средств защиты информации в ИС

6.1. Для создания резервной копии конфиденциальной информации, обрабатываемой в ИС, используются только учтенные (зарегистрированные) в установленном порядке носители информации.

6.2. Ведущий инженер-программист обязан осуществлять резервное копирование конфиденциальной информации, в том числе содержащей персональные данные, с периодичностью, регламентированной ОРД и технологией обработки информации в ИС.

6.3. Перед резервным копированием необходимо проверить носитель информации на отсутствие вредоносных программ.

6.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

6.5. Запрещается запись посторонней информации на учтенные носители информации, предназначенные для копирования персональных данных.

6.6. Ответственность за проведение резервного копирования в ИС возлагается на ведущего инженера-программиста.

6.7. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения возлагается на ведущего инженера-программиста.

6.8. Ответственность за проведение мероприятий по восстановлению работоспособности средств защиты информации (далее - СЗИ) возлагается на ведущего инженера-программиста.

6.9. При использовании для резервного копирования персональных данных, к носителям информации предъявляются следующие требования:

6.9.1. Носители информации, содержащие персональные данные, подлежат учету (регистрации);

6.9.2. Все носители персональных данных, в том числе бумажные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых (при необходимости) шкафах (сейфах). При этом должны быть созданы условия, обеспечивающие их сохранность.

7. Правила антивирусной защиты ИС

7.1. Организация антивирусной защиты возлагается на ведущего инженера-программиста.

7.2. К использованию на АРМ ИС допускаются только лицензионные антивирусные средства.

7.3. Установка и начальная настройка средств антивирусного контроля на АРМ ИС может осуществляться специализированными организациями, а также ведущим инженером-программистом.

7.4. Ведущий инженер-программист осуществляет обновление антивирусных баз с периодичностью, установленной порядком проведения антивирусного контроля или в соответствии с рекомендациями производителя.

7.5. Настройка антивирусных программных средств должны предусматривать проверку на наличие вредоносных программ в начале работы в режиме автозагрузки всех информационных ресурсов АРМ.

7.6. Файлы, помещаемые в электронный архив на носителях информации, должны в обязательном порядке подвергаться антивирусной обработке. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

7.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки программного обеспечения компьютера или внесения в него изменений, ведущим инженером-программистом должна быть выполнена антивирусная проверка ИС.

7.8. При выявлении признаков наличия на АРМ вредоносных программ (нештатная работа программного обеспечения, появление графических и звуковых эффектов, искажений данных, немотивированная утрата массивов данных, частое появление сообщений о системных ошибках и т.п.) пользователь обязан известить об этом ведущего инженера-программиста.

8. Организация парольной защиты в ИС

8.1. Организация процессов генерации паролей, а также контроль периодичности смены паролей, а также прекращения их действия во всех подсистемах ИС возлагается на ведущего инженера-программиста.

8.2. Генерация паролей осуществляется с учетом следующих требований:

- персональный пароль должен содержать не менее 6 символов;
- в числе символов пароля могут использоваться буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего;
- пользователь не имеет права сообщать личный пароль другим лицам.

8.3. Полная смена паролей пользователей должна проводиться регулярно не реже одного раза в полгода.

8.4. В случае прекращения полномочий пользователя (увольнение, смена исполняемых функций внутри СахОДБ и т.п.) внеплановая смена личного пароля или удаление учетной записи пользователя должны производиться ведущим инженером-программистом, с внесением изменений в разрешительную систему доступа ИС.

9. Аудит обращений к информационным ресурсам ИС

9.1. С целью выявления фактов несанкционированного доступа к конфиденциальной информации в ИС система защиты информации в ИС должна предусматривать подсистему аудита обращений.

9.2. Право настройки электронных журналов, а также проверки и контроля обращений к ИС, имеет ведущий инженер-программист.

10. Правила обновления общесистемного и прикладного программного обеспечения ИС, а также технического обслуживания

10.1. Организация обновления (модификации) общесистемного и прикладного программного обеспечения, технического обслуживания возлагается на ведущего инженера-программиста.

10.2. Изменения в конфигурацию аппаратно-программных средств защиты информации, входящих в состав ИС, осуществляется ведущим инженером-программистом с внесением соответствующих отметок в организационно-распорядительные документы ИС. Работы производятся с ведома должностного лица, ответственного за эксплуатацию данной ИС.

10.3. Все изменения конфигураций технических и программных средств должны производиться на основании заявок должностных лиц, ответственных за эксплуатацию ИС.

10.4. Заявка на внесение изменений в конфигурацию системных и прикладных программных средств, входящих в состав ИС, может предусматривать установку (развертывание), обновление, а также удаление на АРМ программных средств, используемых для решения задач ИС;

10.5. Решение, по существу содержащихся в заявке предложений с учетом мнения ведущего инженера-программиста принимает директор СахОДБ.

10.6. Установка и обновление программного обеспечения на АРМ производится только с оригинальных лицензионных дистрибутивных носителей, полученных в установленном порядке, прикладного программного обеспечения – с эталонных копий программных средств.

10.7. При возникновении ситуаций, требующих передачи компонент АРМ, входящего в состав ИС, специализированной сервисной организации для ремонта и обслуживания, носители информации, содержащие персональные данные, извлекаются и помещаются для хранения в специально отведенное для этих целей хранилище (сейф). Носители информации,

извлеченные из системных блоков АРМов, и содержащие персональные данные выносу за пределы СахОДБ не подлежат.

11. Осуществление контроля состояния защиты информации в ИС

11.1. Контроль состояния защиты информации в ИС - проверка организационных и технических мероприятий, предпринятых для обеспечения безопасности персональных данных при обработке в ИС, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

11.2. Основными мероприятиям по контролю состояния защиты информации в ИС являются:

- проверка соответствия условий эксплуатации ИС требованиям нормативных правовых и организационно-распорядительных документов по защите информации в ИС;
- выявление возможных каналов утечки информации и внешних программно-технических воздействий на информацию, обрабатываемую в ИС;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИС от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите всех компонент ИС;
- оперативное принятие мер по пресечению нарушений требований и норм защиты информации в ИС.

11.3. Контроль защиты информации осуществляется с учетом реальных условий эксплуатации ИС как непосредственно на АРМах ИС, в том числе с применением средств аудита обращений к ИС, так и путем ознакомления с организационно-распорядительными документами на ИС.

11.4. С целью проверки эффективности применения организационных и технических мероприятий по защите информации могут проводиться необходимые инструментальные исследования и расчеты с привлечением специалистов специализированной организации, обладающей соответствующими лицензиями на право проведение указанных работ.

11.5. Основными видами технического контроля на объекте организации являются визуальный контроль условий эксплуатации объектов информатизации, контроль эффективности защиты информации от утечки по

техническим каналам, контроль эффективности защиты от несанкционированного доступа к информации и программно-технических воздействий на информацию.

11.6. Невыполнение установленных нормативных требований по защите персональных данных считается предпосылкой утечки (утраты) защищаемой информации.

11.7. В случае выявления предпосылок утечки (утраты) защищаемой информации с целью установления обстоятельств их возникновения может проводиться служебное расследование.

11.8. Контроль защиты информации осуществляется путем проведения как плановых, так и внеплановых проверок объектов защиты. Плановые проверки проводятся не реже одного раза в год.

11.9. Обследование объектов информатизации проводится с целью определения соответствия объектов информатизации ИС требованиям по защите информации. В ходе обследования объектов информатизации проверяется:

- соответствие класса ИС условиям, сложившимся на момент проверки;
- выполнение требований предписаний на эксплуатацию технических средств и систем, организации электропитания и заземления;
- соответствие выполняемых в ИС мероприятий по защите информации данным, изложенным в организационно-распорядительной документации;
- выполнение требований по защите автоматизированных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты;
- наличие электробытовой, радиотелевизионной и иной аппаратуры, которые могут способствовать возникновению каналов утечки информации.

11.10. Государственный контроль состояния защиты информации вправе осуществлять федеральные уполномоченные органы в соответствии с действующим законодательством Российской Федерации.

12. Ответственность должностных лиц

12.1. Должностные лица СахОДБ, допущенные к обработке персональных данных в ИС, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.