Модуль автоматизированного рабочего места центра регистрации читателей
(АРМ «Центр регистрации читателей»)

Пояснительная записка

Модуль автоматизированного рабочего места центра регистрации читателей (АРМ ЦРЧ) разработан для приведения САБ ИРБИС в соответствие требованиям закона Российской Федерации 152-ФЗ «О персональных данных».

Введение

Законодательные требования по обеспечению безопасности персональных данных.

Определения

ИСПДн (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 или без использования таких средств (152-ФЗ, ст.3, п.9)

ПДн (персональные данные) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных); (152-ФЗ, ст. 3, п.1)

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 (152-ФЗ, ст. 3, п.2)

Обезличивание - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных (152_ФЗ, ст. 3., п.8).

Категория ПНд. Для целей классификации ИСПДн вводятся категории персональных данных (Приказ от 13 февраля 2008 года № 55/86/20, ФСТЭК РФ, ФСБ РФ, Министерство информационных технологий и связи РФ)

категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4 - обезличенные и (или) общедоступные персональные данные

Объем обрабатываемых персональных данных Для целей классификации ИСПДн объем обрабатываемых персональных данных (Хпдн) может принимать следующие значения (Приказ от 13 февраля 2008 года № 55/86/20, ФСТЭК РФ, ФСБ РФ, Министерство информационных технологий и связи РФ)

1 - в информационной системе одновременно обрабатываются персональные данные более чем 100000 субъектов персональных данных или персональные данные

субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Класс ИСПДн.

По результатам анализа исходных данных типовой информационной системе присваивается один из следующих классов:

класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Нормативный порядок обеспечения безопасности персональных данных при автоматизированной обработке:

Порядок обеспечения безопасности персональных данных определен постановлением Правительства от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных".

Детализация действий, определенных постановлением Правительства, содержится в методических материалах ФСТЭК.

В соответствии со сложившейся нормативной базой операторам необходимо:

- Описать и классифицировать ИСПДн;
- Разработать модель угроз;
- Разработать проект системы защиты;
- Реализовать меры защиты;
- Оценить соответствие системы защиты требованиям безопасности.

Государственный контроль за соблюдением прав субъектов персональных данных.

Государственный контроль за соблюдением прав субъектов персональных данных возложен на Федеральную Службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (РОСКОМНАДЗОР).

Порядок проведения проверок операторов определен приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 1 декабря 2009 г. № 630 «Об утверждении Административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»

Обеспечение безопасности персональных данных, обрабатываемых в центре регистрации читателей САБ ИРБИС.

Концепция функционирования САБ ИРБИС в защищенном режиме.

Методическим приемом, позволяющим реорганизовать обработку персональных данных, содержащиеся в САБ ИРБИС, с целью оптимизации системы защиты, является обезличивание.

В соответствии концепцией обезличивания САБ ИРБИС разделяется на два сегмента.

Первый сегмент – Центр Регистрации Читателей (ЦРЧ). Этот сегмент представляет собой автономный АРМ и содержит персональные данные читателей в полном объеме. Этот сегмент относится к ИСПДн класса К2 и подлежит защите в соответствии с нормативными требованиями Регуляторов.

Второй сегмент – это модули САБ ИРБИС, обеспечивающие все функции обслуживания читателей и содержащие только номера читательских билетов. В соответствии с правилами классификации этот сегмент является ИСПДн класса К4 и не требует обеспечения конфиденциальности.

Информационное взаимодействие сегментов организуется путем регулярного переноса номеров читательских билетов из сегмента ЦРЧ в сегмент обслуживания читателей с помощью специально отведенного для этих целей USB-флеш-накопителя.

Типовой Центр Регистрации Читателей

Функцией ЦРЧ является регистрация читателей и организация выдачи читательских билетов.

Типовой Центр Регистрации Читателей представляет собой автономный компьютер, расположенный в контролируемой зоне, исключающей несанкционированный доступ посторонних лиц. Доступ в контролируемую зону разрешен только уполномоченным сотрудникам. Контролируемой зоной может являться служебное помещение, проникнуть в которое без применения технических средств посторонним лицам невозможно.

В ЦРЧ обрабатываются персональные данные второй категории, то есть позволяющие идентифицировать субъектов и получить о них дополнительную информацию. Объем обрабатываемых персональных данных составляет более 1 000, но не превышает 100 000 записей о субъектах ПДн (читателей).

В соответствии нормативными документами Регуляторов ЦРЧ является ИСПДн класса К2, не имеющей подключения к ЛВС и сетям общего пользования (Интернет).

Средством переноса номеров читательских билетов из ЦРЧ в обезличенный сегмент САБ ИРБИС является USB-флеш-накопитель. Приказом № 58 ФСТЭК « Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» установлено, что в отношении съемных носителей информации должен быть организован их учет и хранение, исключающие хищение, подмену и уничтожение. Для этого USB-флеш-накопитель, применяемый для переноса номеров читательских билетов в обезличенный сегмент САБ ИРБИС должен быть соответствующим образом промаркирован. Хранение USB-флеш-накопителя должно производится в месте, исключающем его использование не уполномоченными лицами, а сами операции с USB-флеш-накопителем должны регистрироваться в специальном журнале.

Модель угроз ЦРЧ

По требованиям обеспечения безопасности, установленным Федеральной Службой по Техническому и Экспортному Контролю (ФСТЭК), для каждой ИСПДн должна разрабатываться модель угроз. В этом документе по методикам ФСТЭК определяется перечень актуальных угроз, которым подвергается соответствующая ИСПДн. Модель угроз является формализованным документом, имеющим установленную структуру.

Для ЦРЧ Ассоциацией Электронных Библиотек и Новых Технологий разработана модель угроз, которая применима в библиотеках, пользующихся САБ ИРБИС и проводящих обезличивание в соответствии с прилагаемыми инструкциями. Разработанная модель угроз согласована со ФСТЭК и содержится в приложении.

Требования по безопасности ЦРЧ

Регуляторами установлены технические и организационные меры защиты применительно к различным классам ИСПДн. Эти меры кроме класса ИСПДн учитывают также и технические характеристики систем.

Средства технической защиты, которые должны быть применены для ЦРЧ в соответствии с установленными в модели актуальными угрозами:

- Средство защиты от несанкционированного доступа (Даллас Лок);
- Средство антивирусной защиты (устанавливаются пользователем самостоятельно);

Организационные меры защиты, которые необходимо осуществить:

- Выделить АРМ, на котором будет установлено ПО ЦРЧ;
- Выделить и промаркировать USB-флеш-накопитель;
- Выделить контролируемую зону для размещения ЦРЧ;
- Выполнить ряд организационно-распорядительных мероприятий, перечень которых приведен в следующем разделе.

Порядок перевода САБ ИРБИС в защищенный режим

Перевод САБ ИРБИС в защищенный режим производится в следующей последовательности.

1. Организационно-распорядительные мероприятия
   - Приказ об определении целей и порядка обработки ПДн в ЧРЦ
   - Приказ о выделении контролируемой зоны и создании ЧРЦ
   - Подписание Акта классификации
   - Приказ об актуализации Модели угроз
   - Назначение сотрудников, уполномоченных обрабатывать ПДн читателей
   - Ознакомление сотрудников с инструкцией по работе с ЧРЦ
   - Подготовка материального обеспечения: выделение автономного АРМ и приобретение USB-флэш-носителя
   - Исполнение программного модуля разделения ИРБИС на два сегмента (в соответствии с прилагаемой инструкцией)

2. Технические меры защиты
   - установка на ЦРЧ антивирусной защиты
   - установка на ЦРЧ средства защиты от несанкционированного доступа (Dallas Lock)

По завершении перевода САБ ИРБИС в защищенный режим следует провести испытания системы защиты ЦРЧ и заполнить декларацию соответствия.

Заключение

В САБ ИРБИС обрабатываются и хранятся персональные данные читателей, поэтому, в соответствии определениями закона 152-ФЗ «О персональных данных», САБ ИРБИС является информационной системой персональных данных (ИСПДн) и подлежит защите в соответствии с нормативными требованиями Регуляторов.

Прием, с помощью которого САБ ИРБИС переводится в защищенный режим работы, заключается в выделении автономного АРМ ЦРЧ, являющегося единственным местом обработки персональных данных. Выполнение всех функций САБ ИРБИС в дальнейшем будет осуществляться только по номерам читательских билетов, без непосредственной обработки персональных данных читателей.

Вследствие выделения автономного АРМ ЦРЧ, где обрабатываются персональные данные читателей и удаления персональных данных на других рабочих местах, САБ ИРБИС разделяется на два сегмента. В первом сегменте, обеспечивающим полный функционал обслуживания читателей, обрабатываются только номера читательских билетов. Этот сегмент не требует специальных мер защиты. Все персональные данные читателей сосредоточены во втором сегменте – автономном рабочем месте, выполняющим функцию регистрации читателей и выдачи читательских билетов.