**3.22. Защита персональных данных**

Подсистема «Защита персональных данных» предназначена для соответствия информационной системы, построенной на основе конфигурации, требованиям Федерального закона № 152-ФЗ от 27.06.2006 «О персональных данных».

**Настройка**

Для внедрения подсистемы «Защита персональных данных» необходимо принять решение по поводу того, какие сущности в конфигурации являются субъектами персональных данных, т. е. к каким сущностям относятся защищаемые персональные данные. Как правило, это такие справочники, как Физические лица, Сотрудники, Контрагенты, Партнеры и др.

Затем необходимо задать состав типов субъектов персональных данных в качестве определяемого типа СубъектПерсональныхДанных.

В общем модуле ЗащитаПерсональныхДанныхПереопределяемый в процедуре ДополнитьДанныеСубъектовПерсональныхДанных описать определение данных субъекта, необходимых для заполнения документа согласия на обработку персональных данных. См. пример реализации этой процедуры в демонстрационной конфигурации.

Если в конфигурации не используется подсистема «Настройки программы», то в рабочем месте администратора программы необходимо разместить обработку ЗащитаПерсональныхДанных и ее команду ЗащитаПерсональныхДанных. См. пример в форме ПоддержкаИОбслуживание обработки ПанельАдминистрированияБСП.

После этого необходимо подключить механизм настройки регистрации доступа к персональным данным, который включает регистрацию событий журнала регистрации типа Доступ.Доступ. Для этого в подсистемах конфигурации определяются процедуры, в которых заполняются сведения о персональных данных и областях персональных данных. Вызовы таких процедур осуществляются из методов, расположенных в переопределяемом общем модуле ЗащитаПерсональныхДанныхПереопределяемый, – ЗаполнитьСведенияОПерсональныхДанных и ЗаполнитьОбластиПерсональныхДанных соответственно.

Описание сведений о персональных данных представляет собой таблицу значений с колонками типа Строка:

● Объект – полное имя объекта метаданных;

● ПоляРегистрации – имена полей регистрации, разделенные запятой. При необходимости задать альтернативные поля их можно перечислить, разделяя символом «|»;

● ПоляДоступа – имена полей доступа, разделенные запятой;

● ОбластьДанных – имя области персональных данных, к которой относятся описываемые сведения (заполнение не обязательно).

Описание областей персональных данных является обязательным, только если при заполнении сведений определена их принадлежность к конкретной области. Описание областей также заполняется в виде таблицы значений с колонками типа Строка:

● Имя – имя области данных (так, как указано в таблице сведений);

● Представление – пользовательское представление области;

● Родитель – данные, в состав которых входит описываемая область.

Логика заполнения сведений о персональных данных и областей должна определяться исходя из состава субъектов персональных данных, а также состава данных информационной базы, относящихся к персональным. Пример такого заполнения см. в процедурах ЗаполнитьСведенияОПерсональныхДанных и ЗаполнитьОбластиПерсональныхДанных общего модуля ЗащитаПерсональныхДанныхПереопределяемый.

События Доступ.Доступ и Доступ.Отказ в доступе выводятся в форме обработки ЗащитаПерсональныхДанных в том случае, если в информационной базе включена их регистрация. При этом следует иметь в виду, что событие Доступ.Отказ в доступе по умолчанию включено.

Для управления регистрацией событий доступа к персональным данным в форме настройки системы необходимо разместить реквизит и элементы для управления:

● добавить реквизит формы ОбластиПерсональныхДанных типа ДеревоЗначений,

● добавить таблицу формы ОбластиПерсональныхДанных, связанную с этим реквизитом.

Разместить вызовы процедур общего модуля ЗащитаПерсональныхДанных:

● в обработчике ПриСозданииНаСервере – ПриСозданииФормыНастройкиРегистрацииСобытий,

● в обработчике ПриЗаписиНаСервере – ПриЗаписиФормыНастройкиРегистрацииСобытий.

Далее необходимо определить место в командном интерфейсе для включения объектов работы с согласиями на обработку персональных данных субъектов:

● журнала СогласияНаОбработкуПерсональныхДанных,

● отчетов СогласияНаОбработкуПерсональныхДанныхДействующие и СогласияНаОбработкуПерсональныхДанныхИстекающие.

**Настройка скрытия персональных данных**

Если в конфигурации не используется подсистема «Настройки программы», то в командном интерфейсе администратора необходимо разместить следующие объекты метаданных:

● константа ДнейДоСкрытияПерсональныхДанныхСубъектов,

● константа ИспользоватьСкрытиеПерсональныхДанныхСубъектов.

См. пример размещения в демонстрационной конфигурации в группе Защита персональных данных формы НастройкиПользователейИПрав обработки ПанельАдминистрированияБСП.

Для отслеживания потребности в получении согласия на обработку персональных данных и отбора ранее скрытых субъектов, в формах списка субъектов (например, физических лиц), определенных в определяемом типе СубъектПерсональныхДанных, необходимо выполнить ряд действий:

1. В обработчике события формы ПриСозданииНаСервере добавить код:

// СтандартныеПодсистемы.ЗащитаПерсональныхДанных

ЗащитаПерсональныхДанных.ПриСозданииНаСервереФормыСписка(ЭтотОбъект, Элементы.Список);

// Конец СтандартныеПодсистемы.ЗащитаПерсональныхДанных

2. В обработчике события формы ОбработкаОповещения добавить:

// СтандартныеПодсистемы.ЗащитаПерсональныхДанных

ЗащитаПерсональныхДанныхКлиент.ОбработкаОповещенияФормыСписка(Элементы.Список, ИмяСобытия);

// Конец СтандартныеПодсистемы.ЗащитаПерсональныхДанных

3. В обработчике события таблицы формы СписокПриПолученииДанныхНаСервере добавить код:

// СтандартныеПодсистемы.ЗащитаПерсональныхДанных

ЗащитаПерсональныхДанных.ПриПолученииДанныхНаСервере(Настройки, Строки);

// Конец СтандартныеПодсистемы.ЗащитаПерсональныхДанных

4. Дополнительно, для управления видимостью субъектов с ранее скрытыми персональными данными добавляется подключаемая процедура:

#Область ОбработчикиКомандФормы

// СтандартныеПодсистемы.ЗащитаПерсональныхДанных

&НаКлиенте

Процедура Подключаемый\_ПоказыватьСоСкрытымиПДн(Команда) Экспорт

ЗащитаПерсональныхДанныхКлиент.ПоказыватьСоСкрытымиПДн(ЭтотОбъект, Список);

КонецПроцедуры

// СтандартныеПодсистемы.ЗащитаПерсональныхДанных

#КонецОбласти

5. Помимо встраивания кода необходимо настроить элементы и свойства формы списка. Расположить на командной панели группу с именем ГруппаПоказыватьСоСкрытымиПДн.

6. Настроить динамический список формы, добавив соответствующее поле и псевдоним:

ВЫРАЗИТЬ(NULL КАК ЧИСЛО(1, 0)) КАК ОтсутствуетСогласие,

7. К запросу динамического списка добавить соединение с таблицей регистра сведений СубъектыДляСкрытияПерсональныхДанных

ЛЕВОЕ СОЕДИНЕНИЕ РегистрСведений.СубъектыДляСкрытияПерсональныхДанных КАК СубъектыСоКрытымиПДн

ПО Справочник\_ДемоФизическиеЛица.Ссылка = СубъектыСоКрытымиПДн.Субъект

И (СубъектыСоКрытымиПДн.Состояние = ЗНАЧЕНИЕ(Перечисление.СостоянияСубъектовДляСкрытия.СкрытиеВыполнено))

ГДЕ

(СубъектыСоКрытымиПДн.Субъект ЕСТЬ NULL

ИЛИ &ПоказыватьСоСкрытымиПДн)

Готовый пример реализации см. в форме списка справочника \_ДемоФизическиеЛица демонстрационной конфигурации.

8. По желанию, для управления местом размещения колонки «Отсутствует требуемое согласие» можно добавить элемент поля таблицы ОтсутствуетСогласие.

Для обновления формы элемента субъекта персональных данных при наступлении события СкрытыПерсональныеДанные в методе  ОбработкаОповещения размещается вызов:

// СтандартныеПодсистемы.ЗащитаПерсональныхДанных

ЗащитаПерсональныхДанныхКлиент.ОбработкаОповещенияФормы(ЭтотОбъект, ИмяСобытия);

// Конец СтандартныеПодсистемы.ЗащитаПерсональныхДанных

Скрытие персональных данных, хранимых в ссылочных метаданных (Справочники, Документы), выполнится при условиях:

● сведения о персональных данных описаны в методах, вызываемых из переопределяемого метода общего модуля ЗащитаПерсональныхДанныхПереопределяемый (см. в документации к подсистеме),

● если субъект персональных данных встречается только в реквизитах объекта метаданных, то обрабатываются все строки табличных частей объекта,

● если ссылка на субъект есть хотя бы в одной табличной части, то для обработки остальных табличных частей, она должна быть и там.

● если строки табличной части содержат данные разных субъектов, то для обработки с отбором по субъекту, он должен быть в реквизитах этой табличной части,

● если в ПоляхДоступа указаны реквизиты объекта («общие») метаданных, то они будут обработаны независимо от того, встречается субъект в реквизитах самого объекта или реквизитах табличных частей объекта.

Необходимо убедиться, что не требуется уточнения ПолейРегистрации и ПолейДоступа в существующих описаниях и пересмотра структуры объектов метаданных:

● убрать из ПолейДоступа путь к «общим» реквизитам объекта метаданных, которые не должны быть обработаны (возможно, удалить реквизиты из метаданных, заменив их в формах на динамически рассчитываемые),

● добавить в обрабатываемую табличную часть реквизит с типом субъекта (см. определяемый тип СубъектПерсональныхДанных), если такой отсутствует, но подразумевается. И указать его в составе ПолейРегистрации.

**Настройка прав доступа пользователей**

Для настройки прав доступа пользователей к инструментам подсистемы «Защита персональных данных» следует использовать роли, приведенные ниже.

Таблица 3.42.

| № | Роли и их назначение |
| --- | --- |
| 1. | ПросмотрЖурналаРегистрации (из подсистемы «Базовая функциональность»)  Право просмотра журнала регистрации |
| 2. | Администрирование (из подсистемы «Базовая функциональность») |

Для доступа к согласиям на обработку персональных данных необходимо создать в конфигурации роли по аналогии с демонстрационными ролями \_ДемоДобавлениеИзменениеСогласийНаОбработкуПерсональныхДанных и \_ДемоЧтениеСогласийНаОбработкуПерсональныхДанных, описать в них текст необходимого ограничения доступа на уровне записей.

Если в форме списка субъектов требуется выделять субъектов, персональные данные которых уничтожены, следует описать доступ к регистру сведений СубъектыДляСкрытияПерсональныхДанных в одной из ролей, используемых для доступа к субъектам персональных данных. Доступ нужно описать и в том случае, если требуется предоставить возможность интерактивного скрытия персональных данных. Для этого в той же роли  необходимо дать доступ к общей команде СкрытьПерсональныеДанныеСубъектов.

**Использование при разработке конфигурации**

**Настройка обмена данными**

Все объекты метаданных подсистемы рекомендуется включать в планы обмена распределенной ИБ (РИБ), планы обмена автономных рабочих мест, а также в планы обмена по правилам конвертации, за исключением следующих метаданных:

● константа  ДнейДоСкрытияПерсональныхДанныхСубъектов,

● константа  ИспользоватьСкрытиеПерсональныхДанныхСубъектов,

● регистр сведений  ОбластиПерсональныхДанных,

● регистр сведений  СубъектыДляСкрытияПерсональныхДанных.

Из планов обмена по правилам конвертации дополнительно исключается:

● регистр сведений СогласияНаОбработкуПерсональныхДанных.

Регистр СубъектыДляСкрытияПерсональныхДанных хранит информацию о датах регламентного скрытия персональных данных субъектов. Актуальность этих дат зависит от полноты данных на узлах, что в общем случае характеризуется наличием/отсутствием документов СогласиеНаОбработкуПерсональныхДанных и ОтзывСогласияНаОбработкуПерсональныхДанных по всем организациям компании. В ходе получения данных, центральным узлом накапливается состав таких документов – оснований. При завершении обмена необходимо выполнить перерасчет дат по этим основаниям, для чего включить в обработчик события ПередЗаписью плана обмена следующий вызов:

● ЗащитаПерсональныхДанных.ПослеЗагрузкиДанных.

См. пример размещения в демонстрационной конфигурации в модуле объекта планов обмена:

● \_ДемоОбменВРаспределеннойИнформационнойБазе,

● \_ДемоАвтономнаяРабота.

В обменах через универсальный формат EnterpiseData при выгрузке данных, зарегистрированных на узле плана обмена, выполняется принудительная выгрузка объектов по ссылкам в том случае, если ранее они не выгружались. Если выгружаемые данные не относятся к источникам персональных данных, но в реквизитах присутствует ссылка на субъект или источник персональных данных, то необходимо позаботиться о том, чтобы такой объект не был выгружен, если он содержит в себе скрытые персональные данные. Это можно сделать на уровне правил обработки данных, воспользовавшись методом ЭтоОбъектСоСкрытымиПерсональнымиДанными программного интерфейса модуля ЗащитаПерсональныхДанных. Пример см. в демонстрационной конфигурации в методе ПОД\_Справочник\_ФизическиеЛица\_Отправка\_ПриОбработке модуля \_ДемоМенеджерОбменаЧерезУниверсальныйФормат.

Необходимо контролировать выгрузку субъекта по ссылке из не источника персональных данных и в правилах обмена. Пример отказа в выгрузке субъекта со скрытыми персональными см. в демонстрационной конфигурации в макете ПравилаОбмена плана обмена \_ДемоОбменСБиблиотекойСтандартныхПодсистем в ПКС свойства ФизическоеЛицо ПКО \_ДемоОтветственныеЛица.