



**SAFE-DOC.COM**

ОНЛАЙН-СЕРВИС ПОДГОТОВКИ ДОКУМЕНТОВ

**Инструкция заполнению информации и  
подготовке первичного пакета документов  
по защите персональных данных**

# Оглавление

ОГЛАВЛЕНИЕ .....	2
ЗАПОЛНЕНИЕ РУБРИКИ <i>ОРГАНИЗАЦИЯ</i> .....	4
<i>Пункт. Общие данные</i> .....	4
Раздел 1. Об организации .....	4
Раздел 2 Структура подразделений.....	6
<b>Раздел 3 Список должностей</b> .....	7
Раздел 4 Список сотрудников.....	7
Раздел 5 Список помещений.....	8
Раздел 6 О руководителе.....	9
<i>Пункт 2 «Ответственные лица и комиссии»</i> .....	10
Раздел 1 Ответственные лица .....	10
Раздел 2 Ответственные отделы .....	11
Раздел 3 Комиссии .....	11
РУБРИКА «МЕРОПРИЯТИЯ» .....	12
<i>Пункт «Стартовые»</i> .....	12
Раздел 1 Сведения конфиденциального характера .....	12
Раздел 2 «Размещение сотрудников» .....	12
Раздел 3 «Информация о серверах».....	13
Раздел 4 Информация о рабочих местах.....	15
Раздел 5 Информационные системы.....	16
Раздел 6 Материальные носители .....	19
Раздел 7 Резервное копирование .....	21
Раздел 8 Контрольные даты .....	22
Раздел 9 Средства криптографической защиты.....	23
<i>Пункт 2 Оперативные</i> .....	24
Раздел 1 Документооборот .....	24
Раздел 2 Кадровые мероприятия .....	24
Раздел 3 Структурные изменения.....	24
Раздел 4 Мероприятия по СКЗИ .....	25
Раздел 5 Повторное формирование пакета документов.....	25
Раздел 6 Ведение журналов.....	25
Раздел 7 Акты .....	25
Раздел 8 Дополнительные документы .....	26
<i>Пункт Модель угроз</i> .....	27
Раздел 1 Лист согласования .....	27
Раздел 2 Технические и эксплуатационные характеристики ИСПДн .....	27
Раздел 3 Угрозы безопасности .....	28
Раздел 4 Формирование .....	30
<i>Пункт Технические решения</i> .....	31
ФОРМИРОВАНИЕ ПАКЕТА.....	31
РУБРИКА ДОКУМЕНТЫ .....	31
Раздел 1 Текущие документы .....	31
Раздел 2 Акты .....	32
Раздел 3 Журналы .....	32
Раздел 4 Архив.....	32

Вход на сервис

Шаг1 На сайт!

Открываем браузер, предпочтительнее Mozilla Firefox. В адресной строке вводим: <https://safe-doc.com/>

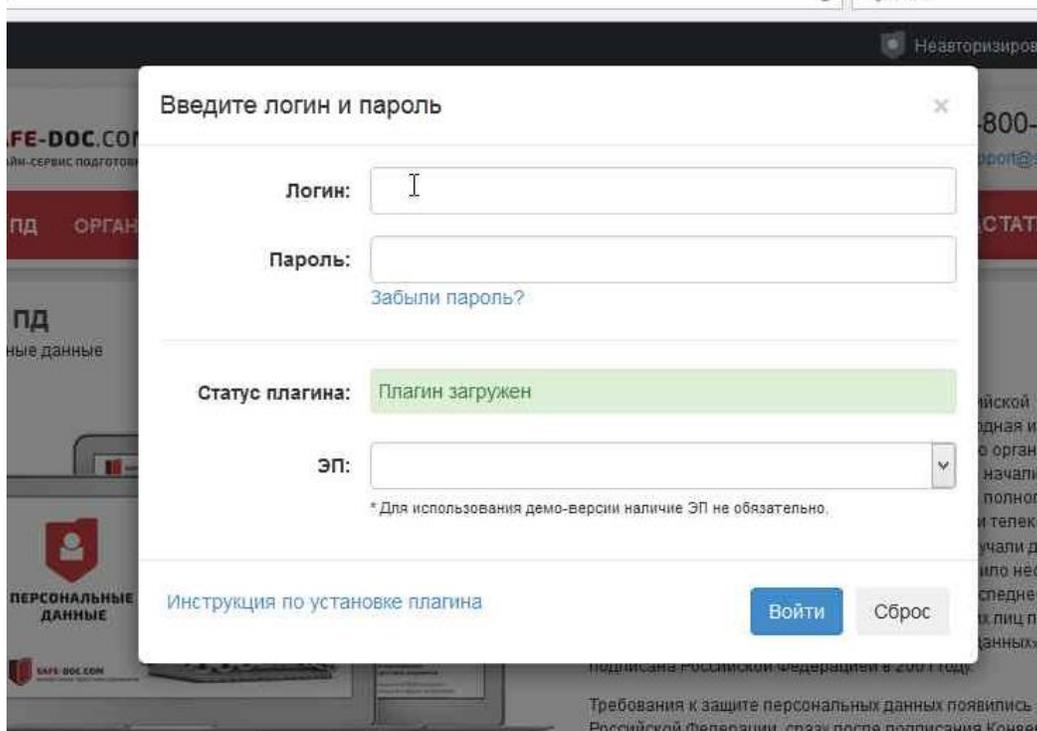
Шаг2 Войти

В правом верхнем углу нажимаем кнопку **Войти**

Шаг3 Окно авторизации

В открывшееся окно авторизации (Рисунок 1) вводим ваш логин (адрес электронной почты, на который Вы зарегистрировались) и пароль. В случае, если Вы привязали ЭП, выберите эту подпись из списка в поле **ЭП**.

*Примечание:* Поле **Статус плагина** необходимо для проверки корректной работы плагина работы с ЭП.



The image shows a login dialog box on a web browser. The dialog has a title bar with the text "Введите логин и пароль" and a close button. It contains the following elements:

- A "Логин:" label followed by a text input field.
- A "Пароль:" label followed by a password input field and a link "Забыли пароль?".
- A "Статус плагина:" label followed by a green bar containing the text "Плагин загружен".
- An "ЭП:" label followed by a dropdown menu.
- A note: "\*Для использования демо-версии наличие ЭП не обязательно."
- A link "Инструкция по установке плагина" on the bottom left.
- Two buttons: "Войти" (blue) and "Сброс" (grey) on the bottom right.

Рисунок 1 Окно авторизации

Шаг4 Стартовое окно

Процедура входа в сервис завершена, перед Вами стартовое окно сервиса(Рисунок 2). В левом верхнем углу указан Ваш тариф, в правом – пользователь, от имени которого Вы вошли.

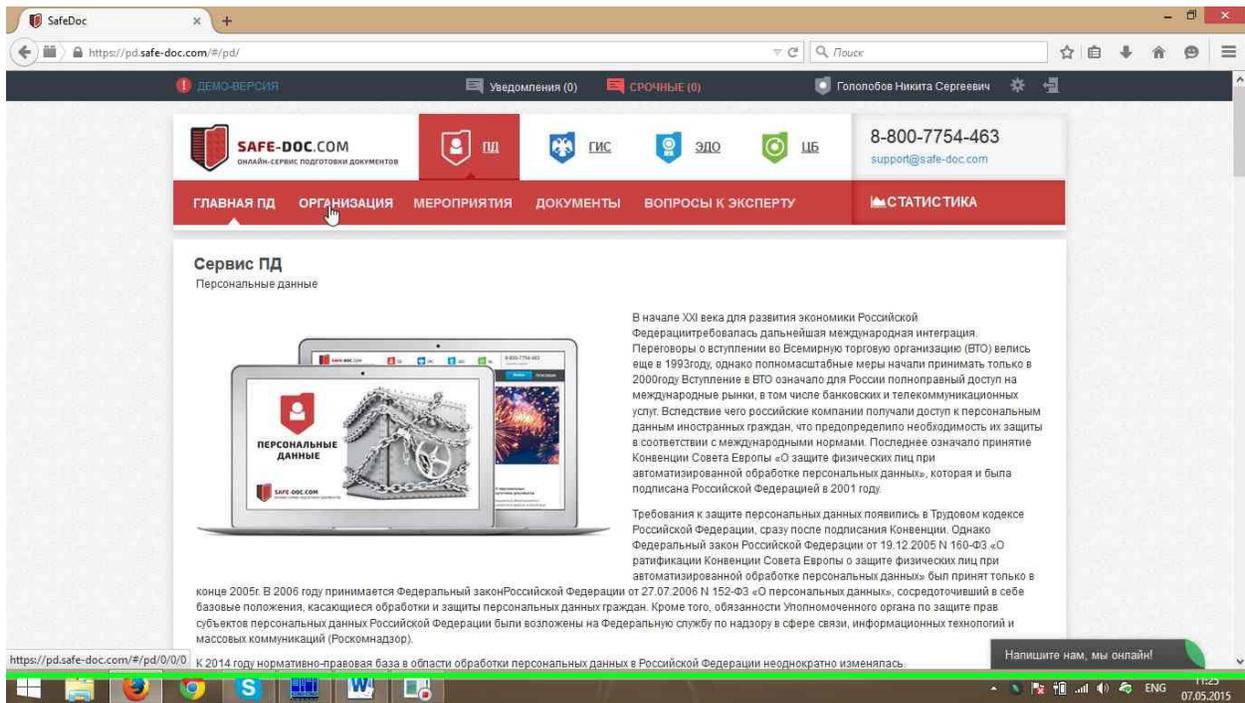


Рисунок 2 Стартовая страница сервиса

## Заполнение рубрики *Организация*

### Пункт. Общие данные

#### Раздел 1. Об организации

##### Шаг 1 К разделу

Переходим в раздел: **Организация->Общие данные->Об организации** (Рисунок 3)

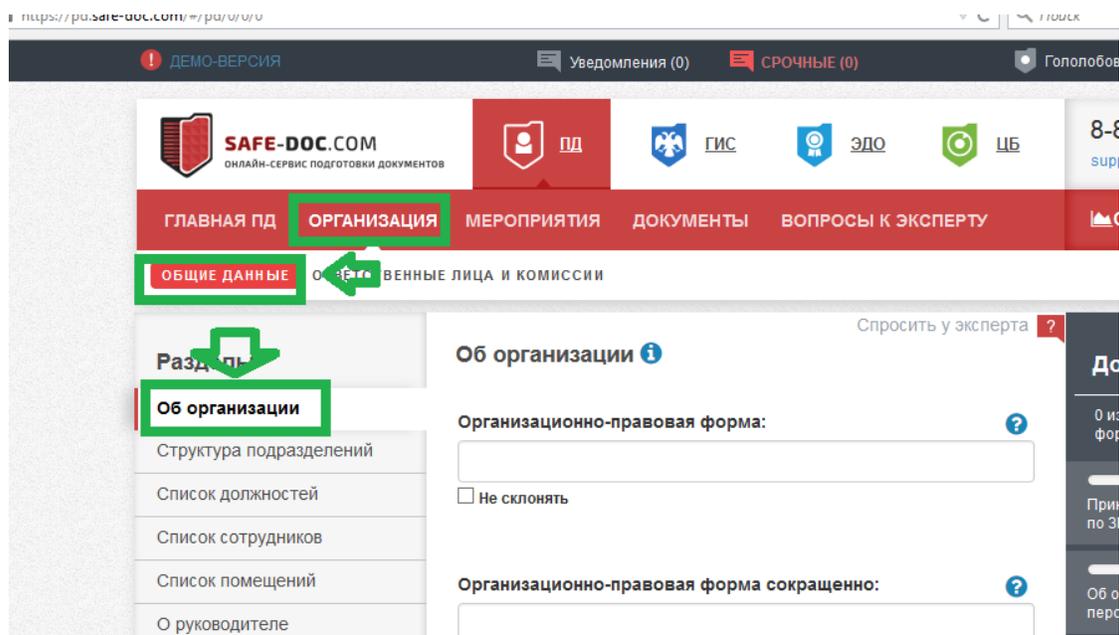


Рисунок 3 Переход в подраздел

## Шаг 2 Организационно-правовая форма

Введите полное официальное наименование организационно-правовой формы (при наличии). Например, Общество с ограниченной ответственностью. Для сохранения проверьте падежные формы, либо установите флажок **Не склонять**, если склонение не требуется.

## Шаг 3 Полное наименование организации

Укажите полное официальное наименование организации без указания организационно-правовой формы (если необходимо, то название нужно указать в кавычках). Например, «Информационные технологии». Для сохранения проверьте падежные формы.

## Шаг 4 Сокращенное наименование организации

Укажите в кавычках сокращенное официальное наименование организации без указания организационно-правовой формы. Например, «ИТ». Для сохранения проверьте падежные формы.

## Шаг 5 ИНН

Укажите индивидуальный налоговый номер организации.

## Шаг 6 Адрес организации

В соответствующих полях укажите индекс и почтовый адрес организации.

## Шаг 7 Тип распорядительного документа

Укажите тип распорядительного документа, используемого в Вашей организации. Это необходимо сделать для корректного формирования шаблонов утверждаемых организационно-распорядительных документов.

## Шаг 8 Дата регистрации юридического лица

Для корректного определения даты начала обработки персональных данных необходимо указать дату регистрации юридического лица.

## Шаг 9 Данные об уведомлении

Если организацией ранее подавалось уведомление в Роскомнадзор, то необходимо указать номер уведомления и дату внесения в реестр. В случае, если уведомление не подавалось, то данные поля заполнять не нужно.

*Примечание:* Если Вы не знаете точно, подавалось ли уведомление, это можно проверить наличие организации в реестре операторов на сайте Роскомнадзора по адресу: <http://rkn.gov.ru/personal-data/register/>

## Шаг 10 Логотип

В случае необходимости можно загрузить логотип либо герб Вашей организации (в формате jpg или png), который будет вставлен во все формируемые распорядительные документы.

## Шаг 11 Далее!

Для перехода к следующему разделу нажмите *Далее*

## Раздел 2 Структура подразделений

Инструментарий сервиса позволяет создать иерархическую структуру подразделений организации, в которых обрабатываются персональные данные.

### Шаг 1 Добавление главного структурного подразделения

Нажимаем кнопку *Добавить новое* (рисунок 4)

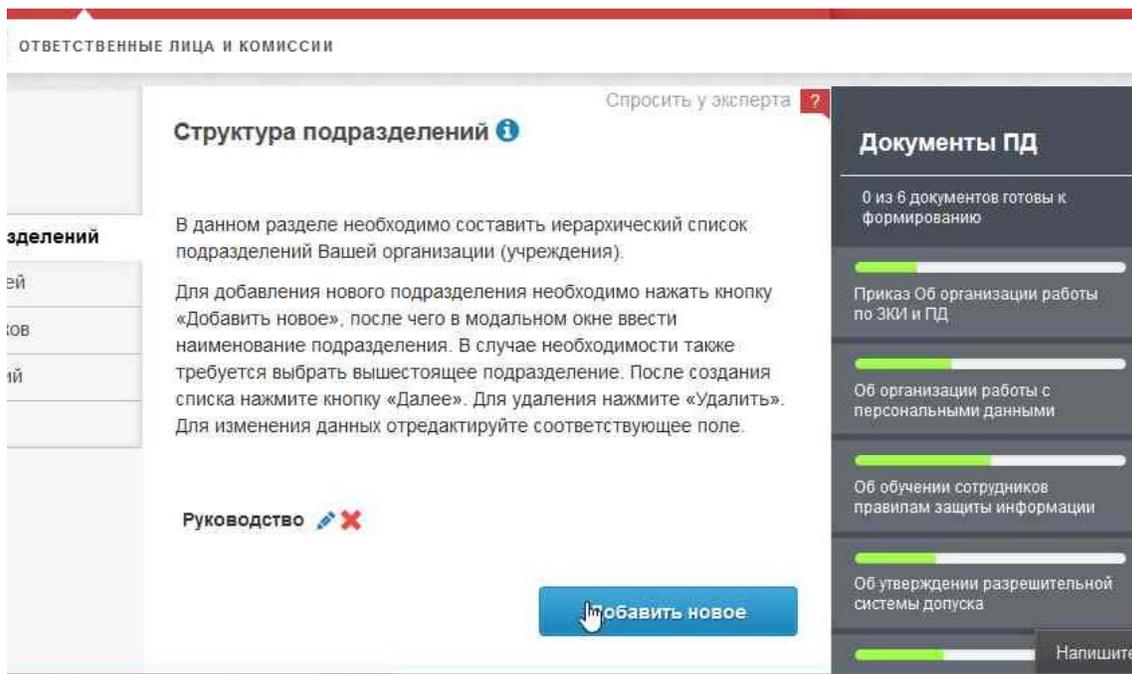


Рисунок 4 Добавление подразделения

### Шаг 2 Информация о добавляемом подразделении

Во всплывающем диалоговом окне (Рисунок 5) необходимо указать информацию о добавляемом подразделении: название с падежными формами, вышестоящее подразделение. В случае, если у добавляемого подразделения нет вышестоящих, установите соответствующую галочку.

Название:

Не склонять

Вышестоящее подразделение отсутствует

Вышестоящее подразделение:

Выберите из списка

Сохранить

Рисунок 5 Окно информации о подразделении

Шаг 3 К следующему разделу

Для перехода к следующему разделу нажмите *Далее*

### Раздел 3 Список должностей

В разделе необходимо добавить все должности, которые занимают сотрудники, осуществляющие обработку персональных данных, а также лица, утверждающие документы и являющиеся ответственными.

Шаг 1 Название должности

Вводим название добавляемой должности, проверяем падежные формы, нажимаем кнопку *Добавить*

Шаг 2 Далее

Для перехода к следующему разделу нажмите *Далее*

### Раздел 4 Список сотрудников

В список необходимо добавить всех сотрудников организации, которые, так или иначе, будут указаны в документах: лица, утверждающие документы, члены комиссий, ответственные за организацию обработки, допущенные к обработке сотрудники и т.д.

Шаг 1 Добавить сотрудника

Для добавления нового сотрудника нажмите *Добавить нового*

Шаг 2 Данные о сотруднике

В открывшемся всплывающем окне (Рисунок 6) введите все необходимые данные о сотруднике: фамилию, имя, отчество с указанием падежных форм, выберите из списка должность и подразделение. Если у сотрудника не требуется указывать подразделение – установите соответствующую галочку.

Добавить сотрудника

Фамилия:  
  
 Не склонять

Имя:  
  
 Не склонять

Отчество:  
  
 Не склонять

Должность:  
Выберите из списка  
 Без подразделения

Подразделение:  
Выберите из списка

Сохранить

Рисунок 6 Окно добавления сотрудника

### Шаг 3 Далее

После добавления всех необходимых сотрудников в список нажмите **Далее** для перехода к следующему разделу

### Раздел 5 Список помещений

В разделе необходимо добавить адреса всех зданий, в которых обрабатываются персональные данные. Для каждого здания нужно указать кабинеты, в которых осуществляется обработка.

### Шаг 1 Добавить адрес

Для добавления нового здания нажмите **Добавить новый адрес**

### Шаг 2 Добавление адреса

В открывшемся диалоговом окне укажите почтовый индекс здания и адрес.

В случае, если электрическая подстанция находится в пределах контролируемой зоны (периметр организации, территория, доступ на которую контролируется организацией), установите соответствующую галочку. Данная информация необходима при моделировании угроз безопасности. В случае, если вы не располагаете данными о расположении подстанции, следует предполагать, что она располагается за пределами контролируемой зоны.

### Шаг 3 К добавлению кабинетов

Следующий шаг предусматривает указание для каждого из адресов (зданий) кабинетов, в которых осуществляется обработка ПДн. Добавление кабинетов осуществляется во всплывающем окне, которое можно открыть нажатием на кнопку **Помещения**.

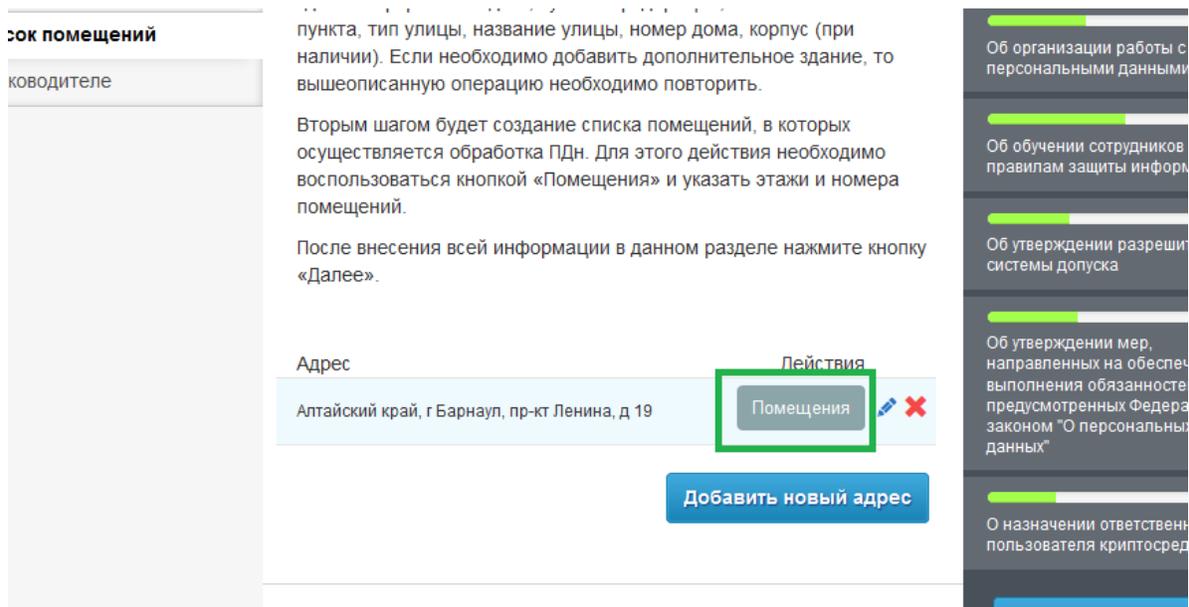


Рисунок 7 Кнопка добавления кабинетов

#### Шаг 4 Добавление кабинетов

Во всплывающем окне добавления кабинетов (Рисунок 8) необходимо для каждого из добавляемых кабинетов указать его номер, этаж и нажать **Добавить**

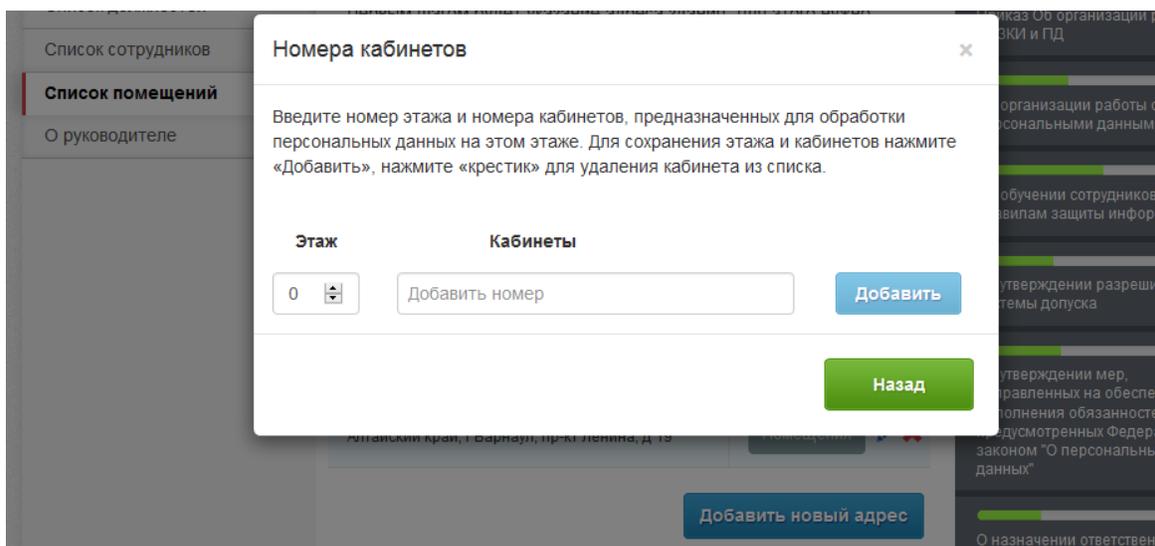


Рисунок 8 Добавление кабинетов

#### Шаг 5 Далее

После добавления всех необходимых в документации зданий и кабинетов нажимаем **Далее** для перехода к следующему разделу

#### Раздел 6 О руководителе

В разделе указывается руководитель, от имени которого в общем случае будут утверждаться документы.

*Примечание.* При формировании пакета документов имеется возможность, при необходимости, для некоторых документов указать другое утверждающее лицо.

## Шаг 1 Выбор руководителя

На странице раздела (Рисунок 9) необходимо выбрать руководителя из списка (список формируется на этапе ввода данных в раздел «*Список сотрудников*»), а также указать, на основании чего он действует.

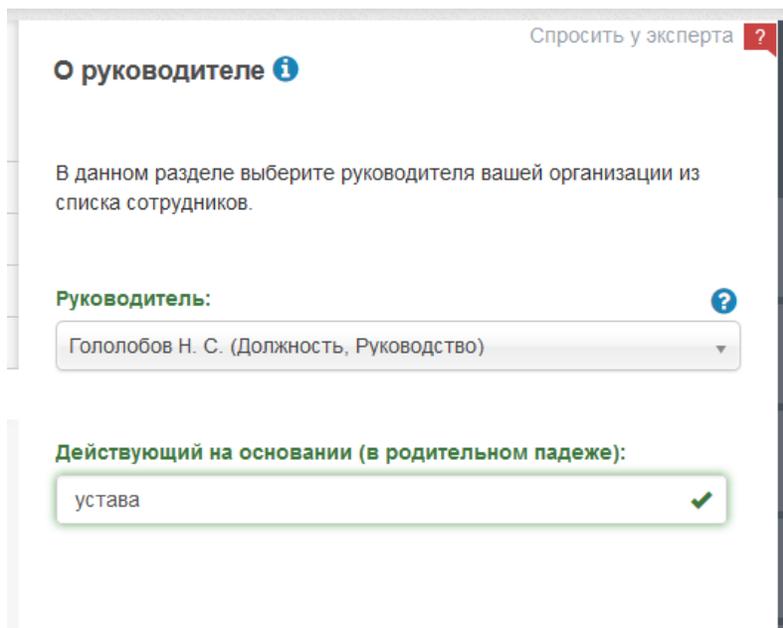


Рисунок 9 Раздел "О руководителе"

## Шаг 2 Далее

Для перехода к следующему пункту рубрики «*Организация*» нажмите *Далее*

## Пункт 2 «Ответственные лица и комиссии»

### Раздел 1 Ответственные лица

В данном разделе необходимо выбрать ответственных из списка сотрудников. В случае отсутствия в списке необходимого сотрудника, вернитесь к разделу «Об организации → Список сотрудников».

*Ответственный за исполнение приказов* – лицо, которое указывается ответственным в приказах, утверждающих нормативные документы. Обычно указывается кто-либо из руководителей.

*Ответственный за ознакомление с приказами* –лицо, на которое возлагается ответственность за проведение ознакомления сотрудников с приказами. Обычно это какой-либо из ответственных лиц в кадровых или организационных подразделениях. Например, сотрудник отдела кадров, офис-менеджер и т.п.

*Ответственный за ПД* – лицо, на которого возлагается ответственность за организацию процесса обработки и защиты персональных данных. Часто в этой роли выступает кто-либо из руководящего состава организации.

*Ответственный за безопасность ПД* – лиц несущее ответственность за безопасность персональных данных. Часто в этой роли выступает руководитель подразделения, сотрудники которого занимаются практическими вопросами обеспечения безопасности ПД.

*Администратор ИБ* – лицо, непосредственно занимающееся практическими вопросами защиты ПД: установка и настройка средств защиты, проверка их работоспособности, ведение журналов выдачи и журналов учета и т.д. Это сотрудник, подчиняющийся ответственному за безопасность ПД. В небольших организациях часто не разделяют эти роли и назначают на них одного и того же человека.

*Ответственный за антивирусную проверку* – лицо, осуществляющее поддержание антивирусной защиты в актуальном и работоспособном состоянии. Обычно это сотрудник подразделения, осуществляющего техническую поддержку средств вычислительной техники

*Ответственный за техническое обслуживание* – лицо, непосредственно осуществляющее техническое обслуживание средств вычислительной техники, либо руководитель подразделения, осуществляющего эти функции.

*Ответственный за криптосредства* – сотрудник, ответственный за исполнение правил работы со средствами криптографической защиты информации.

*Заместитель ответственного за криптосредства* – сотрудник, замещающий ответственного за криптосредства. Согласно требованиям ФСБ, замещающее лицо должно быть обязательно назначено.

#### Шаг 1 Ответственные лица

Выберите всех ответственных лиц из списка сотрудников

#### Шаг 2 Далее

Для перехода к следующему разделу нажмите *Далее*

#### Раздел 2 Ответственные отделы

*Отделы, ответственные за обеспечение функционирования информационных систем* – отдел или отделы, осуществляющий техническое обслуживание вычислительной техники. В случае отсутствия такого отдела, укажите должность ответственного сотрудника (например, системный администратор)

*Отделы, ответственные за кадровое обеспечение* – кадровое подразделение или подразделения. В случае отсутствия такого отдела, укажите должность ответственного сотрудника (например, специалист по кадрам)

*Должность руководителя отдела, ответственного за кадровое обеспечение* – руководитель подразделения, осуществляющего прием на работу и увольнение. Данный сотрудник согласует заявки на предоставление и прекращение доступа сотрудников к информационным системам. В случае отсутствия такого отдела, укажите должность ответственного сотрудника (например, специалист по кадрам).

*Отделы, ответственные за обеспечение собственной безопасности* – подразделение или подразделения, осуществляющее контроль физического доступа в контролируемую зону, а так же осуществляющее(ие) охрану зданий. В случае отсутствия такого отдела (например, отдел внутреннего контроля), укажите должность ответственного сотрудника (например, инспектор службы безопасности).

#### Шаг 1 Заполнение информации об отделах

Заполните все необходимые поля, выбрав из списков.

#### Шаг 2 Далее

Нажмите *Далее* для перехода к следующему разделу

#### Раздел 3 Комиссии

Все действия по уничтожению персональных данных, допуску к работе со средствами криптографии, определению уровней защищенности должны выполняться комиссионно с оформлением итогового документа (акта). В организации должны быть созданы следующие комиссии:

*Комиссия по установлению уровней защищенности* – определяет уровень защищенности информационных систем персональных данных исходя из категории обрабатываемых данных, их количества, угроз безопасности и некоторых других моментов.

*Комиссия по уничтожению материальных носителей* – комиссия, актирующая уничтожение материальных носителей (персональных данных на бумажных носителях).

*Комиссия по уничтожению электронных носителей* – комиссия, актирующая уничтожение электронных носителей (персональных данных на жестких дисках, флэш-носителях и т.д.).

*Комиссия по допуску к самостоятельной работе с СКЗИ* – комиссия, которая актом допускает сотрудников, после успешного прохождения обучения, к самостоятельной работе о средствами криптографической защиты.

## Шаг 1 Комиссии

Выберите лиц, возглавляющих и входящих в комиссии. Один сотрудник может входить в несколько комиссий. В состав комиссии должно входить не менее двух человек.

## Шаг 2 Далее

Для перехода к следующей рубрике нажмите *Далее*

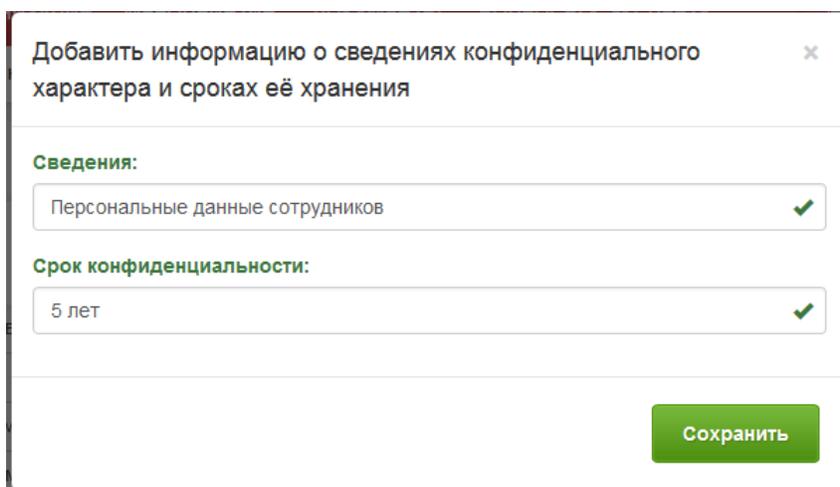
## Рубрика «Мероприятия»

### Пункт «Стартовые»

#### Раздел 1 Сведения конфиденциального характера

##### Шаг 1 Добавление категории

Нажатием на кнопку **Добавить** открываем диалоговое окно добавления категории конфиденциальной информации (Рисунок 10)



The screenshot shows a dialog box titled "Добавить информацию о сведениях конфиденциального характера и сроках её хранения". It contains two input fields: "Сведения:" with the value "Персональные данные сотрудников" and "Срок конфиденциальности:" with the value "5 лет". Both fields have a green checkmark on the right. A green "Сохранить" button is located at the bottom right of the dialog.

Рисунок 10 Добавление категории конфиденциальной информации

Срок конфиденциальности - срок в течении которого следует хранить конфиденциальную информацию согласно целям обработки. По истечении срока обработки данные должны быть переданы в архив, если это требуется, либо уничтожены. Обработка персональных данных по достижении целей обработки или по истечении срока обработки не допускается!

## Шаг 2 Далее

Для перехода в следующую рубрику нажмите *Далее*

#### Раздел 2 «Размещение сотрудников»

В данном разделе необходимо указать, в каком кабинете работает каждый из указанных в «Списке сотрудников». Для этого выберите из списка необходимого сотрудника и для него выберите из списка кабинеты, в которые он имеет доступ. При этом предполагается, что один сотрудник может иметь доступ в несколько кабинетов.

Под доступом понимается право сотрудника находиться в помещении без присутствия других лиц.

## Шаг 1 Размещение сотрудников

Выберите одного или несколько сотрудников из списка, выберите кабинет, в котором он работает. Нажмите **Добавить**

1, 1 этаж (пр-кт Ленина 19): Гололобов Н.С.	Удалить
2, 1 этаж (пр-кт Ленина 19): Пупкин В.И.	Удалить

**Сотрудники, имеющие доступ:** ?

Выберите из списка

**Кабинет:**

Выберите из списка Добавить

Рисунок 11 Доступ сотрудников в помещения

*Примечание:* Если у вас нет нужных кабинетов в списке, значит Вам нужно вернуться в раздел 5 «Список помещений» и добавить недостающие кабинеты.

## Шаг 2 Далее

Нажмите **Далее** для перехода в следующий раздел.

## Раздел 3 «Информация о серверах»

В разделе необходимо добавить все используемые для обработки персональных данных сервера.

В случае, если обработка осуществляется на рабочем месте пользователя, указывать данный компьютер как сервер не следует.

## Шаг 1 Добавление сервера

Для добавления сервера нажмите **Добавить**. Откроется диалоговое окно добавления сервера (Рисунок 12).

Редактировать информацию о сервере

Наименование: 1с-server

Назначение: терминальный сервер

Модель: hp dl380 g8

Серийный (инвентарный) номер: 0001

Объем оперативной памяти: 4096 МБ

Операционная система: Windows Server 2008 Standard Edition 32Bit

Сведения о сертификации:

Прикладное программное обеспечение:

Рисунок 12 Добавление сервера

## Шаг 2 Информация о сервере

В открывшемся диалоговом окне необходимо некоторые данные.

Данные, позволяющие идентифицировать сервер в генерируемых документах:

- Наименование – название сервера, которое будет отражено в генерируемых документах.
- Назначение – для чего используется сервер. Например, терминальный сервер, сервер виртуализации, файловый сервер и т.п.
- Модель – модель используемого сервера.
- Серийный (инвентарный) номер.

Техническая информация о сервере:

- Объем оперативной памяти: объем указывается в мегабайтах, либо гигабайтах.
- Используемая операционная система(ОС): используемую операционную систему необходимо выбрать из списка. В случае, если вашей ОС нет в списке, сообщите нам – исправим ☺. Если у Вас используется сертифицированная ФСТЭК версия ОС (в наличии сертифицированный дистрибутив с формулярами и голографической наклейкой), укажите сведения о сертификации в соответствующее поле.
- Используемое прикладное программное обеспечение: какие программы помимо операционной системы и средств защиты (в случае, если таковые уже имеются) установлены, либо могут быть установлены на данный сервер: архиватор, файловый менеджер, просмотрщики графики, офисный пакет и т.д.

Информация об имеющихся средствах защиты:

- Антивирусное ПО: выберите из списка используемый у вас антивирус. Если необходимого антивируса нет в списке, сообщите нам - исправим. В случае, если у Вас используется сертифицированная ФСТЭК версия антивирусного ПО (в наличии сертифицированный дистрибутив с формулярами и голографической наклейкой), укажите сведения о сертификации в соответствующее поле.

- Средство защиты от несанкционированного доступа – Если у на Вашем сервере уже установлено сертифицированное средство защиты, укажите его.

- Межсетевой экран – Если у Вас уже используется сертифицированный межсетевой экран, укажите его.

*Примечание:* Напомним, что средство защиты считается сертифицированным ФСТЭК, когда у Вас имеется специальный дистрибутив с комплектом необходимой документации: формуляр, голографическая наклейка ФСТЭК, копия актуального сертификата. Для сертифицированных ФСБ средств защиты требования аналогичны, за исключением голографической наклейки.

Прочая необходимая информация о сервере:

- Имя домена: при использовании домена можно указать его имя.
- Требования к паролю: требования, которые применяются при выборе и смене паролей пользователей на сервере, а также периодичность его смены (например, «ежеквартально»).
- Сетевой адрес: адрес, по которому сервер доступен во внутренней сети, адрес по которому можно получить доступ к его ресурсам, в том числе и для резервного копирования.
- Группы пользователей, имеющих доступ: например, «администраторы», «пользователи 1С».
- Кабинет: местоположения сервера. Если необходимого кабинета нет в списке, его необходимо добавить на шаге 4 в разделе «Список помещений».

По завершению заполнения информации о сервере нажмите **Сохранить**

### Шаг 3 Далее

Для перехода в следующий раздел нажмите **Далее**

### Раздел 4 Информация о рабочих местах

В разделе заполняется информация о компьютерах ( рабочих станциях), на которых осуществляется обработка персональных данных.

#### Шаг 1 Добавление рабочей станции

Для добавления рабочей станции необходимо нажать **Добавить**

#### Шаг 2 Информация о рабочей станции

В открытом диалоговом окне необходимо заполнить некоторую информацию о рабочей станции:

- Наименование: название рабочей станции.
- Серийный (инвентарный) номер: номер, по которому можно рабочую станцию однозначно идентифицировать.
- Объем оперативной памяти: укажите размер физической памяти.
- Операционная система: выберите из списка. Если операционная система сертифицирована, то указать сведения о сертификате.
- Прикладное программное обеспечение: разрешенное к использованию и уже используемое на рабочей станции ПО
- Антивирус: выберите из списка. Если антивирус сертифицирован, то указать сведения о сертификате.
- Средство защиты от несанкционированного доступа: если уже используется сертифицированное средство от НСД.
- Программный межсетевой экран: при наличии сертифицированного межсетевого экрана.



- Название домена: имя домена, в случае использования
- Парольная политика: требования к сложности пароля, его длине и частоте смены
- Пользователи: пользователи, которые имеют доступ к рабочей станции.

### Шаг 3 Сохранить

После заполнения всех необходимых данных нажмите **Сохранить**

### Шаг 4 Далее

После добавления всех рабочих станций для перехода в следующий раздел нажмите **Далее**

## Раздел 5 Информационные системы

В разделе необходимо заполнить информацию об информационных системах, в которых обрабатываются персональные данные.

### Шаг 1 Наименование ИСПДн

Укажите полное наименование информационной системы и проверьте падежные формы

### Шаг 2 Объем ПДн

Укажите, какой объем персональных данных (персональные данные какого количества субъектов) обрабатывается в информационной системе

### Шаг 3 Категория субъектов

Укажите категорию субъектов персональных данных: сотрудники оператора, или не сотрудники. В случае если имеются и те и другие, то указывать следует «Не сотрудники»

### Шаг 4 Типы актуальных угроз

Выберите из списка, какого типа угрозы актуальны для данной информационной системы

Угрозы 1-го типа актуальны для информационной системы, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

### Шаг 5 Способ уничтожения

Способ уничтожения данных: укажите каким способом будет уничтожаться данные, например, затиранием.

### Шаг 6 Документ о вводе ИС

Реквизиты документа о вводе информационной системы в эксплуатацию: указывается при наличии. Например, приказ о создании, вводе в эксплуатацию и т.п.

### Шаг 7 Актуальность конфиденциальности

Установите галочку, если для информационной системы актуальны требования конфиденциальности (неразглашения, предотвращения несанкционированного доступа)

## Шаг 8 Допущенные к ИСПДн

Сотрудники, имеющие доступ: выберите из списка сотрудников, допущенных к данной информационной системе.

## Шаг 9 Добавить данные о субъекте

Данные о категории субъектов персональных данных. Для добавления категории субъектов нажмите **Добавить данные**. Откроется окно добавления категории субъектов (Рисунок 13)

Добавить данные о категории субъектов ПД

Категория субъектов персональных данных: ?

Не склонять

Категория обрабатываемых персональных данных:

Выберите из списка

Состав обрабатываемых персональных данных:

Добавить

Цели обработки:

Добавить данные

Источники информации: ?

Добавить

Получатели информации: ?

Добавить

Сохранить

Рисунок 13 Добавление категории субъектов

## Шаг 10 Категория субъектов

Категория субъектов персональных данных: Название категории, например, «сотрудники».

## Шаг 11 Категория ПДн

Категория обрабатываемых персональных данных: категория персональных данных, обрабатываемых в информационной системе:

- специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;
- биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

- общедоступные персональные данные - персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных";
- иные категории персональных данных – персональные данные, не относящиеся ни к одной из перечисленных выше категорий персональных данных.

## Шаг 12 Состав обрабатываемых ПДн

Состав обрабатываемых персональных данных: укажите какие персональные данные обрабатываются в информационной системе. Например, фамилия, паспортные данные, сведения об образовании и т.п.

## Шаг 13 Цели обработки

Цели обработки: необходимо добавить одну или несколько целей обработки персональных данных. Для добавления нажмите **Добавить данные**

Рисунок 14 Добавление цели обработки персональных данных

**Цель:** название цели обработки

**Правовые основания:** законы, распоряжения Правительства, и другие нормативные документы, во исполнение которых обрабатываются персональные данные. Правовым основанием также является договор, стороной которого или выгодоприобретателем является субъект персональных данных.

**Срок обработки и хранения:** Сроки в течении которых достигаются цели обработки, либо утрачивают силу правовые основания обработки персональных данных.

## Шаг 14 Источники информации

Источники информации: укажите, от кого получены персональные данные

## Шаг 15 Получатели информации

Получатели информации: укажите, куда персональные данные субъектов передаются, например, ПФР, Налоговая служба и т.д.

По завершении, для сохранения и перехода к следующему шагу нажмите **Сохранить**

## Шаг 16 Данные об архитектуре ИС

Данные о серверной части: выберите сервер из списка. Если данные обрабатываются на ПК локально, то указывать сервер не нужно.

Данные о рабочих местах: Выберите из списка рабочие места, на которых обрабатываются персональные данные.

## Шаг 17 Тип ИСПДн

Выберите по какому типу организована ИС:

- Клиент-серверное приложение (приложение, подключающееся при работе к серверу и использующее его ресурсы)
- Локальное приложение (приложение запускаемое на рабочем ПК)

#### Шаг 18 Адрес ИСПДн

Укажите из списка адреса, где находится ИСПДн

#### Шаг 19 Рабочие места в пределах КЗ

Отметьте, находятся ли рабочие места в пределах контролируемой зоны

#### Шаг 20 Структура ИСПДн

Укажите структуру ИСПДн: локальная (все рабочие места объединены в локальную сеть) или распределенная (рабочие места или локальные сети соединяются с помощью технологий удаленного доступа)

#### Шаг 21 Подключение к сетям общего пользования

Имеются подключения к сетям связи общего пользования, например, к сети Интернет.

#### Шаг 22 Режим обработки ПДн

Выберите режим обработки:

- многопользовательский
- однопользовательский

#### Шаг 23 Разграничение прав

Укажите, имеются ли разграничения прав доступа (разный набор прав для разных пользователей)

#### Шаг 24 Далее

После добавления всех информационных систем, нажмите *Далее* для перехода к следующему разделу

### Раздел 6 Материальные носители

#### Шаг 1 Добавление

Для добавления данных о материальных носителях персональных данных нажмите *Добавить*

Рисунок 15 Добавление данных о материальных носителях

### Шаг 2 Заполнение данных о материальных носителях

Введите следующую информацию о материальных носителях:

Наименование: название категории обрабатываемых материальных носителей

Кабинет: выберите из списка кабинет, в котором обрабатываются и хранятся материальные носители

Место хранения: например сейф, закрываемый шкаф и т.д.

Объем записей о субъектах персональных данных:

- Менее 100000
- Более 100000

Способ уничтожения данных: например, сжигание, измельчение.

Сотрудники, имеющие доступ: выберите сотрудников, имеющих доступ к материальным носителям

### Шаг 3 Категория субъектов

Для добавления данных о категориях субъектов персональных данных на материальных носителях нажмите **Добавить данные**

Добавить данные о категории субъектов ПД ×

---

Категория субъектов персональных данных: ?

Не склонять

Категория обрабатываемых персональных данных:

Выберите из списка ▼

Состав обрабатываемых персональных данных:

Цели обработки:

Источники информации: ?

Получатели информации: ?

---

Рисунок 16 Категория субъектов ПД на материальных носителях

#### Шаг 4 Заполнение информации о категории субъектов

В открывшемся окне (Рисунок 16) заполните следующие данные:

- Категория субъектов персональных данных: название категории
- Категория обрабатываемых персональных данных: специальные, биометрические, общедоступные, иные.
- Состав обрабатываемых персональных данных: например, ФИО, должность, паспорт и т.д.
- Цели обработки: аналогично целям для электронных носителей (Шаг 13)
- Источники информации: например, субъекты
- Получатели информации: кому носители передаются?

#### Шаг 5 Далее

Для перехода к следующему разделу нажмите *Далее*

### Раздел 7 Резервное копирование

#### Шаг 1 Добавить информацию о РК

Нажмите *Добавить*, чтобы добавить информацию о резервном копировании информационной системы (Рисунок 17)

Добавить информацию о резервном копировании ×

Место расположения резервной копии: ?

Информационная система:  
 Выберите из списка ▼

Источники копирования:

Ответственный за резервное копирование: ?  
 Выберите из списка ▼

Срок хранения резервной копии: ?

Периодичность копирования: ?

Средство осуществления резервного копирования: ?

Рисунок 17 Добавление информации о резервном копировании

Место расположения резервной копии: куда производится копирование

Информационная система: для которой выполняется копирование

Источники копирования: откуда осуществляется резервное копирование

Ответственный за резервное копирование: кто отвечает за выполнение копирования

Срок хранения резервной копии: сколько копии хранятся. Рекомендуется иметь минимум три разных копии данных

Периодичность копирования: определяется исходя из критичности потери информации за определенный период

Средство осуществления резервного копирования: каким способом, либо с помощью чего осуществляется копирование

## Шаг 2 Далее

После добавления информации о резервном копировании для всех информационных систем нажимаем *Далее* для перехода к следующему разделу

## Раздел 8 Контрольные даты

В разделе необходимо задать контрольные даты исполнения плановых мероприятий по защите информации.

Можно задать периодически повторяющиеся мероприятия. О наступлении плановой даты мероприятия оператор будет уведомлен сообщением в системе, а также по электронной почте.

### Шаг 1 Дата мероприятий по установлению уровня защищенности

Выберите дату, которой будет утверждаться акты определения уровня защищенности

### Шаг 2 Мероприятия по защите информации

Нажмите Добавить, для добавления в план нового мероприятия по защите. При нажатии открывается окно добавления (Рисунок 18)

Рисунок 18 Добавление мероприятия по защите

### Шаг 3 Внутренняя проверка условий обработки персональных данных

Добавить мероприятие по внутреннему контролю. Мероприятие рекомендуется проводить ежегодно. При добавлении необходимо заполнить форму аналогично Рисунку 18.

### Шаг 4 Мероприятия по устранению недостатков

В случае недостатков, выявленных при внутренней проверке, необходимо обозначить сроки устранения недостатков.

### Шаг 5 Мероприятия по техническому обслуживанию

Задайте мероприятия по техническому обслуживанию средств вычислительной техники.

## Раздел 9 Средства криптографической защиты

В разделе необходимо добавить средства криптографической защиты( шифрования) информации (СКЗИ). Средством криптографической защиты называется средство защиты, на которое есть соответствующий сертификат ФСБ, данное средство защиты должно использоваться для защиты персональных данных.

### Шаг 1 Данные на СКЗИ

Наименование: название средства защиты

Производитель: производитель средства защиты

Регистрационный номер: регистрационный номер в реестре ФСБ. Он указан в формуляре на СКЗИ.

### Шаг 2 Список пользователей

Список пользователей: перечень лиц, использующих данное СКЗИ

### Шаг 3 Перечень помещений

Список помещений, выделенных для установки СКЗИ и хранения ключевых документов к ним: список помещения, в которых данное СКЗИ используется, а также в которых хранятся ключевые документы к нему (сертификаты, ключи шифрования).

### Шаг 4 Далее

Нажмите **Сохранить** и **Далее** для перехода к следующему разделу

## Пункт 2 Оперативные

### Раздел 1 Документооборот

В разделе существует возможность подготовить приказ о признании недействительным предыдущих приказов. В приказ добавятся все необходимые реквизиты предыдущих документов.

На первоначальном этапе( при формировании первичного пакета документов) заполнять данный раздел не нужно. Инструмент помогает отменить только приказы, сгенерированные с помощью сервиса.

#### Шаг 1 Выберите приказ

Выберите приказ, который необходимо аннулировать в поле **Приказы, которые необходимо признать утратившими силу**

#### Шаг 2 Основание

Впишите основание признания приказа недействительным. Например, в связи со сменой названия организации, в связи с Постановлением Правительства и т.д.

#### Шаг 3 Утвердить приказ

Нажмите **Утвердить приказ**, чтобы сформировать приказ об отмене.

#### Шаг 3 Далее

Для перехода к следующему шагу нажмите **Далее**

### Раздел 2 Кадровые мероприятия

В разделе содержатся инструменты для облегчения корректировки документов в связи с кадровыми изменениями:

- изменение данных о сотруднике,
- изменение ответственного сотрудника,
- изменения в составах комиссий.

При всех этих изменениях имеется возможность внести их во все нужные места в документах и утвердить обновленные версии только необходимых документов.

#### Шаг 1 Внесение изменений

Внесите необходимые изменения, например в состав комиссий.

#### Шаг 2 Утверждение

Нажмите **Утвердить**, для подготовки необходимых измененных документов.

#### Шаг 3 Далее

Для перехода на следующий этап нажмите **Далее**

### Раздел 3 Структурные изменения

В разделе имеются инструменты для внесения оперативных изменений в уже утвержденный пакет документов.

Можно добавить новый адрес и кабинеты, данные об информационных системах, и аппаратных ресурсах, на которых они выполняются. Будут подготовлен набор новых версий только тех документов, в которые требуется внести изменения.

#### Шаг 1 Внесение изменений

Внесите необходимые изменения, например, добавьте адрес.

#### Шаг 2 Внести

Нажмите **Внести изменения** для подготовки необходимых документов



### Шаг 3 Далее

Для перехода к следующему разделу нажмите *Далее*

### Раздел 4 Мероприятия по СКЗИ

В раздел обладает функционалом аналогичным предыдущим разделам. Инструменты раздела позволяют внести изменения, связанные с эксплуатацией СКЗИ. Изменить можно: данные об СКЗИ, комиссию по допуску к самостоятельной работе с СКЗИ.

#### Использование

Внесите необходимые изменения и нажмите **Внести изменения** для подготовки документов

### Раздел 5 Повторное формирование пакета документов

Раздел позволяет произвести повторное формирование первичного пакета документов. Формирование первичного пакета документов происходит в общем случае один раз, в дальнейшем с помощью сервиса вносятся изменения в этот пакет. При этом ведется корректно история изменений в приказах. Повторное формирование может понадобиться при смене названия организации, смене нумерации приказов.

*Примечание* Логикой работы сервиса не предусмотрено повторное формирование стартового пакета без наличия оснований на это. При отправке запроса необходимо это основание указать, чтобы эксперт имел возможность на основании данного вами разъяснения (в окне отправке запроса) принять решение о подтверждении либо отклонении запроса.

#### Использование

Нажмите **Отправить запрос** для запроса на повторное формирование пакета документов

### Раздел 6 Ведение журналов

В данном разделе собраны журналы, утвержденные нормативными документами разрабатываемые нашим сервисом.

Все журналы доступны для ведения в электронном виде. В любой момент вы можете выгрузить сведения из интересующего вас журнала для ознакомления с содержащейся в нём информацией и дальнейшей печати.

Для начала работы необходимо создать список журналов, которые вы намерены вести, и присвоить каждому журналу номер. Для этого выберете из списка журнал, который Вы хотите создать, и в отобразившемся окне укажите его номер. Если журнал уже создан, то вы сразу перейдёте к содержащимся в нём сведениям.

#### Шаг 1 Добавление журнала

Нажимаем Создать, открывается диалоговое окно добавления журнала

#### Шаг 2 Номер журнала

Выбираем, какой журнал нужно вести и указываем его номер

#### Шаг 3 Далее

После добавления всех необходимых журналов нажмите *Далее*

*Примечание:* Ведение журналов в электронном виде с помощью сервиса не обязательно.

### Раздел 7 Акты

В данном разделе содержатся все необходимые инструменты для изменения документов, связанных с кадровым составом Организации.

- Обязательство о неразглашении сведений конфиденциального характера – подготовка обязательства на конкретного сотрудника. После подготовки обязательства его нужно будет только выгрузить и утвердить.

- Парольная карта – парольная карта пользователя. Подготавливается при необходимости выполнить резервное копирование пароля пользователя
- Заявка на внесение изменений в состав аппаратно-программных средств ИС – заявка необходима для документирования внесения изменений в конфигурации информационных систем: замена компьютера, его частей и т. п.
- Акт об удалении информации (остаточной), хранившейся на диске компьютера – подготавливается комиссионно при уничтожении информации.
- Акт установки оборудования – акт установки оборудования и ввода его в использование.
- Акт установления уровня защищенности информационной системы персональных данных – акты установления уровня защищенности (согласно Постановлению Правительства №1119)
- Акт об удалении (уничтожении) персонализированных записей из информационных систем персональных данных – оформляется при удалении записей с персональными данными
- Заявление о согласии на обработку персональных данных
- Заявление на создание (продление) учетной записи пользователя
- Заявление на изменение полномочий пользователя
- Заявление на блокировку учетной записи пользователя
- Акт ввода в эксплуатацию средств криптографической защиты информации – акт ввода в эксплуатацию СКЗИ
- Протокол проведения внутренней проверки условий обработки ПДн – оформляется по результатам внутренней проверки состояния защищенности оператором. Проверка осуществляется согласно плану проведения внутренних проверок.
- Заключение о допуске к самостоятельной работе с средствами криптографической защиты информации – заключение оформляется комиссионно по результатам прохождения сотрудником программы обучения
- Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные – оформляется в случае отказа субъекта в предоставлении ПДн
- Уведомление об уничтожении персональных данных – направляется субъекту при уничтожении его персональных данных
- Уведомление об устранении нарушений – оформляется при устранении нарушений, направляется субъекту
- Уведомление субъекта об обработке его персональных данных – уведомление готовится в случае, если персональные данные получены не непосредственно от субъекта.
- Заявление об ознакомлении с информацией – заявление, которое заполняет субъект для ознакомления со своими ПДн
- Отметка об исполнении заявления субъекта персональных данных – оформляется при исполнении запроса субъекта
- Карточка данных об инциденте информационной безопасности – заполняется при выявлении инцидента информационной безопасности

## Раздел 8 Дополнительные документы

С помощью инструментария данного раздела можно сформировать:

- план контролируемой зоны,
- перечень должностей, отвечающих за проведение мероприятий по обезличиванию – оформляется при проведении мероприятий по обезличиванию
- документ о наделении правом пользования электронной подписью – оформляется, если сотрудники пользуются чужой ЭП, например ЭП руководителя или главного бухгалтера.

## Пункт Модель угроз

### Раздел 1 Лист согласования

#### Шаг 1 Выбор ИС

Выберите информационную систему из списка

#### Шаг 2 Выбор лиц

Выберите из списка:

- Лицо, составившее модель угроз.
- Лицо, утверждающее модель угроз.
- Лицо, согласовывающее модель угроз.

#### Шаг 3 Далее

Для перехода к следующему разделу нажмите *Далее*

### Раздел 2 Технические и эксплуатационные характеристики ИСПДн

#### Шаг 1 Выберите ИСПДн

Выберите ИСПДн из списка

#### Шаг 2 Территориальное размещение

Укажите, какой является ИСПДн по территориальному размещению:

- Распределенная – охватывает несколько областей, краев, округов.
- Городская – охватывает не более одного города.
- Корпоративная – охватывает многие подразделения предприятия.
- Локальная (кампусная) – в пределах нескольких корпусов, близко расположенных зданий.
- Локальная – в пределах одного здания

#### Шаг 3 Укажите, какой является ИСПДн по подключению к сетям общего пользования:

- Многоточечный доступ – несколько подключений к Интернету или другим сетям общего пользования
- Одноточечный доступ – одно подключение к Интернету или другим сетям общего пользования
- Без доступа – нет подключения к сетям общего пользования, в том числе Интернет

#### Шаг 4 ИСПДн по встроенным операциям

Укажите какие встроенные операции допустимы в ИСПДн:

- Чтение, поиск
- Запись, удаление, сортировка
- Модификация, передача

#### Шаг 5 Круг лиц, имеющих доступ

Укажите кто имеет доступ к ИСПДн (может легально выполнять предусмотренные в ИСПДн операции)

- Открытый доступ к ИСПДн
- Только строго установленный перечень сотрудников организации
- Любые сотрудники организации

#### Шаг 6 Интеграция

Укажите, имеется ли интеграция баз ИСПДн другими базами, не принадлежащими организации

## Шаг 7 Обезличивание

Укажите, обезличиваются персональные данные, если да, то в каких случаях:

- Всегда обезличиваются
- Обезличиваются при передаче в другие организации
- Никогда не обезличиваются

## Шаг 8 Предоставление ПДн сторонним пользователям

Укажите, предоставляются ли персональные данные сторонним лицам и в каком объеме:

- Предоставляется вся база
- Предоставляется часть базы
- Ничего не предоставляется

## Шаг 9 Далее

Нажмите далее для перехода к следующему разделу

## Раздел 3 Угрозы безопасности

### Шаг 1 Выберите ИС

Выберите ИСПДн, для которой будет составляться модель угроз

### Шаг 2 Актуальность угроз

Для каждой из представленных угроз оцените, насколько она реализуема (актуальна) в условиях вашей организации. Напомним, что актуальность угроз определяется оператором самостоятельно.

*Просмотр информации на дисплее пользователей ИСПДн работниками, не допущенными к ПДн*

Угроза актуальна при условии, что в помещение имеют доступ не допущенные сотрудники, причем мониторы расположены таким образом, что позволяют считывают не допущенными сотрудника информацию с экрана.

*Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн*

Аналогично предыдущей угрозе, но определяется в отношении лиц, не являющихся сотрудниками организации.

*Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, ведущими наблюдение (регистрацию) за пределами контролируемой зоны*

При определении актуальности следует учитывать расположение экранов мониторов относительно оконных проемов, а также наличие преград для рассматривания сквозь окна (шторы, жалюзи).

*Просмотр информации на дисплеях пользователей ИСПДн с помощью специальных устройств регистрации, внедренных в помещение, в котором ведется обработка ПДн*

Угроза реализуема в случае, если у злоумышленника есть доступ в помещение для установки специальных устройств снятия информации с дисплея.

*Утечка информации по сетям электропитания ИСПДн*

Угроза актуальна в случае выхода линий электропитания за пределы контролируемой зоны ( трансформаторная подстанция не в пределах контролируемой зоны)

*Перехват техническими средствами наводок информативного сигнала, обрабатываемого техническими средствами ИСПДн, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны*

Угроза актуальна при наличии доступа злоумышленника к линиям связи и электропитания. А также отсутствия на этих линиях устройств развязки и фильтрации

*Утечка информации из ИСПДн за счет побочного излучения технических средств*

Утечка актуальна при наличии ПЭМИН, с уровнем выше уровня естественного шума. Угрозу предлагается считать неактуальной для всех случаев, кроме тех где это отдельно оговорена в требованиях к защищенности (государственные информационные системы).

#### *Преднамеренное электромагнитное воздействие на элементы ИСПДн*

Злоумышленник должен иметь доступ к элементам ИСПДн, доступ в контролируемую зону.

#### *Перехват управления загрузкой операционной системы ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления несанкционированного доступа к ПДн*

Наличие физического доступа к элементам ИСПДн для установки отчуждаемых носителей, а также управления ходом загрузки.

#### *Вызов штатных программ ИСПДн или запуск специально разработанных программ, реализующих несанкционированный доступ к ИСПДн*

Злоумышленник должен располагать правами на запуск(вызов) штатных программ, а также на установку новых программ, реализующих несанкционированный доступ.

#### *Внедрение в ИСПДн вредоносного программного обеспечения*

Актуально при наличии уязвимостей в программном обеспечении

#### *Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации*

Актуально при наличии доступа злоумышленника к каналам связи. Для этого злоумышленник должен иметь к ним доступ в пределах контролируемой зоны, либо каналы должны выходить за ее пределы.

#### *Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей*

Угроза актуальна при подключении ИСПДн к сетям общего пользования, либо при наличии доступа в контролируемую зону у злоумышленника.

#### *Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа*

Актуально при наличии доступа злоумышленника к доверенным каналам передачи информации, а также при наличии уязвимости в программном обеспечении, реализующем сетевые протоколы. Говорить о наличии уязвимостей нужно при отсутствии обновлений безопасности.

#### *Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных*

Для реализации необходимо наличие уязвимостей в сетевых протоколах, позволяющих произвести навязывание ложного маршрута. Говорить о наличии уязвимостей нужно при отсутствии обновлений безопасности.

#### *Внедрение ложного объекта сети*

Злоумышленнику необходим доступ к доверенным каналам передачи данных. В сети должны отсутствовать средства контроля доступа к сети, либо в этих средствах присутствуют уязвимости (нет обновлений безопасности).

#### *Сетевые атаки типа «Отказ в обслуживании»*

Наличие уязвимостей в прикладном и системном ПО, реализующем функции сетевого взаимодействия. Наличие у злоумышленника достаточных ресурсов для проведения атаки.

#### *Удаленный запуск приложения в ИСПДн*

Наличие у злоумышленника прав на удаленный запуск приложений. Наличие уязвимостей в прикладном ПО, позволяющих осуществить удаленный запуск.

#### *Внедрение по сети вредоносного программного обеспечения*

Отсутствие проверки запускаемого ПО. Наличие уязвимостей в сетевых протоколах, позволяющих осуществить внедрение вредоносного ПО.

#### *Хищение носителей информации, содержащих ПДн*

Физический доступ к носителям информации лиц не допущенных к обработке. Отсутствие учета носителей информации

#### *Вывод из строя элементов ИСПДн*

Наличие физического доступа в элементам ИСПДн

#### *Внедрение в ИСПДн аппаратных закладок*

Отсутствие контроля состава аппаратных средств.

#### *Утрата паролей доступа к ИСПДн*

Хранение паролей на материальных носителях. Халатное отношение к хранению паролей

#### *Искажение или уничтожение информации в результате ошибок пользователя*

Халатность, невнимательность пользователя

#### *Выход из строя аппаратно-программных средств ИСПДн*

Устаревшие материально-технические средства с истекшим сроком эксплуатации. При отсутствии жестких требований к времени восстановления работоспособности угроза может быть признана неактуальной.

*Загрузка сторонней операционной системы (без средств защиты и разграничения доступа к ресурсам компьютера)*

Присутствие сторонних носителей со сторонними ОС. Наличие возможности загрузки с отчуждаемого носителя. Физический доступ к элементам ИСПДн.

#### *Сбой системы электроснабжения ИСПДн*

Отсутствие систем резервирования электропитания. Наличие жестких требований к отказам в работе элементов ИСПДн.

*Уничтожение данных в ИСПДн или блокирование доступа к ИСПДн, вызванное стихийными бедствиями или техногенными катастрофами*

Непреднамеренные действия пользователей, вызывающие техногенные последствия: организовал короткое замыкание, затопил серверную и т.п.

### Шаг 3 Далее

Для перехода в следующий раздел нажмите **Далее**

### Раздел 4 Формирование

Для формирования модели угроз нажмите **Сформировать модель угроз**

#### Шаг 1 Формирование

Если у Вас заполнены все необходимые данные в разделах пункта **Модель угроз**,

то в данном разделе напротив имени информационной системы будет доступна кнопка **Сформировать модель угроз**. Нажмите на нее для запуска процесса формирования.

**Примечание:** сформированная модель угроз находится в рубрике пункте **Текущие документы** рубрики **Документы**.

Шаг 2 Далее

Для перехода к следующему разделу нажмите *Далее*

## Пункт Технические решения

Данный пункт находится в разработке

## Формирование пакета

После заполнения всей необходимой информации можно приступить к формированию первичного пакета документов. Пакет можно сформировать нажатием на кнопку **Сформировать пакет**. После запуска процесса формирования необходимо указать номера приказов.

*Примечание:* Номера приказов необходимо указывать реальные. Смена номеров приказов возможно только при регенерации стартового пакета. Повторная генерация стартового пакета возможна только через запрос к экспертам сервиса и получения от них подтверждения(Пункт 2 раздела 5)

## Рубрика Документы

### Раздел 1 Текущие документы

The screenshot shows the 'Текущие документы' (Current Documents) section of the SAFE-DOC.COM website. At the top, there is a navigation bar with the logo 'SAFE-DOC.COM' and the tagline 'ОНЛАЙН-СЕРВИС ПОДГОТОВКИ ДОКУМЕНТОВ'. To the right of the logo are icons for 'ПД' (PD), 'ГИС' (GIS), 'ЭДО' (EDR), and 'ЦБ' (CB). Further right, the contact information '8-800-7754-463' and 'support@safe-doc.com' is displayed. Below the navigation bar, there are tabs for 'ГЛАВНАЯ ПД', 'ОРГАНИЗАЦИЯ', 'МЕРОПРИЯТИЯ', 'ДОКУМЕНТЫ', 'ВОПРОСЫ К ЭКСПЕРТУ', and 'СТАТИСТИКА'. Under the 'ДОКУМЕНТЫ' tab, there are sub-tabs for 'ТЕКУЩИЕ ДОКУМЕНТЫ', 'АКТЫ', 'ЖУРНАЛЫ', 'ОТЧЕТЫ', and 'АРХИВ'. The main content area is titled 'Текущие документы' and includes a checkbox for 'Показывать отменённые' and a link for 'Выделенные в архив'. A button 'Выгрузить последние документы' is also present. Below this, there is a list of documents. The first document is 'Приказ Об организации работы по ЗКИ и ПД №1 от 10.02.2016 г.' with a 'W pdf' icon and a date dropdown set to '7-2016-04-26'. A link '? Вопрос эксперту' is visible below the document title. A button 'Показать приложения (31)' is located below the first document. The second document is 'Об организации работы с персональными данными №2 от 10.02.2016 г.' with a 'W pdf' icon and a date dropdown set to '7-2016-04-26'. A link '? Вопрос эксперту' is also visible below this document title.

Рисунок 19 Раздел текущие документы

На рисунке приведен раздел **Текущие документы** в нем содержатся сформированные Вами приказы, приложения, а также модель угроз.

Все приведенные в данном разделе документы доступны для загрузки как каждый в отдельности, так и все последние версии документов сразу.

Для загрузки конкретного документа нажмите на один из значков, обозначенных на рисунке цифрой 3. В зависимости от того какой значок Вы нажали документ выгрузится в формате DOCX (Microsoft Word), либо PDF.

Для загрузки последних версий всех документов нажмите **Выгрузить последние документы** (обозначены цифрой 1).

Для того чтобы выгрузить какую-то из старых версий документа, выберите необходимую версию из списка (на рисунке обозначено цифрой 2)

## Раздел 2 Акты

В разделе отражаются все сформированные акты: акты определения уровня защищенности, акты уничтожения и т.д.

Инструментарий раздела аналогичен предыдущему.

## Раздел 3 Журналы

В разделе отображаются журналы, которые ведутся с помощью сервиса, и в которых есть записи. Данный раздел позволяет выгрузить журналы.

## Раздел 4 Архив

В разделе хранятся устаревшие и признанные утратившими силу версии документов. Имеющиеся документы можно выгрузить для ознакомления. Никак других действий с данными документами произвести невозможно.