**Техническое задание**

на предоставление неисключительных (пользовательских) прав на программное обеспечение для управления процессами и мероприятиями по защите информации

# **Общие положения**

# Описание услуг разработано с целью определения Заказчиком (далее – Заказчик) состава и содержания услуг по предоставлению Заказчику неисключительных (пользовательских) прав на программное обеспечение для управления процессами и мероприятиями по защите информации.

# **Используемые сокращения**

|  |  |  |
| --- | --- | --- |
| ИСПДн | − | Информационная система персональных данных |
| КИИ | − | Критическая информационная инфраструктура |
| НПА | − | Нормативный правовой акт |
| ОКИИ | − | Объект критической информационной инфраструктуры |
| ПДн | − | Персональные данные |
| Роскомнадзор | − | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций |
| СЗИ | − | Средство защиты информации |
| СКЗИ | − | Средство криптографической защиты информации |
| ФСБ России | − | Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | − | Федеральная служба по техническому и экспортному контролю Российской Федерации |

# **Цель и правовые основания оказания услуг**

# Целями оказания услуг являются:

* обеспечение безопасности ПДн, обрабатываемых Заказчиком, в соответствии с действующим законодательством Российской Федерации в области обработки и защиты ПДн;
* обеспечение безопасности ОКИИ Заказчика в соответствии с действующим законодательством Российской Федерации в области обеспечения безопасности КИИ.

# Правовые основания для оказания услуг:

* Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
* Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
* Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
* Постановление Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»;
* Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
* Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
* Методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 5 февраля 2021 г.

# **Состав, описание и содержание услуг, требования к документированию**

# Исполнитель обязан оказать услуги в составе и объеме, указанном в таблице 1.

Таблица 1

| **№**  **п/п** | **Состав и объем услуг** | **Отчетная документация** |
| --- | --- | --- |
|  | Передача неисключительных (пользовательских) прав на программное обеспечение для управления процессами и мероприятиями по защите информации, в соответствии с п. 4.2 | * Акт приема-передачи прав; * Лицензионный/сублицензионный договор |

# Исполнитель должен передать Заказчику неисключительные (пользовательские) права на программное обеспечение для управления процессами и мероприятиями по защите информации (далее – Программа для ЭВМ) в составе, указанном в таблице 2, с учетом требований к функционалу, указанному в п. 4.3.

Таблица 2

| **№**  **п/п** | **Наименование** | **Состав лицензии** | **Кол-во, шт.** |
| --- | --- | --- | --- |
|  | Программа для ЭВМ. Клиентская лицензия на срок 1 (один) год | Состав лицензии:   * клиентская лицензия с функционалом: * реализация мер по обеспечению безопасности объектов КИИ в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ, постановления Правительства Российской Федерации от 08.02.2018 № 127, приказа ФСТЭК России от 22.12.2017 № 236; * реализация мер по обеспечению безопасности ПДн в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ, постановлений Правительства Российской Федерации от 01.11.2012 № 1119, от 15.09.2008 № 687, приказа ФСТЭК России от 18.02.2013 № 21, приказа ФСБ России от 10.07.2014 № 378 | 1 |

# Требования к Программе для ЭВМ

# Программа для ЭВМ должна быть построена по клиент-серверной архитектуре, где в качестве клиентской части на рабочем месте пользователя выступает веб-браузер.

# На момент предоставления неисключительных (пользовательских) прав Программа для ЭВМ должна иметь следующие функциональные возможности:

* внесение сведений:
  + об организации;
  + ресурсах организации;
  + особенностях обработки ПДн;
  + особенностях функционирования ИСПДн, ОКИИ;
* описание реализуемых организационных и технических мер по обеспечению безопасности ПДн;
* описание ролевой модели системы разграничения доступа;
* управление пользовательскими стилями в документации;
* генерация и выгрузка документации;
* выгрузка форм документов;
* оценка угроз безопасности информации;
* формирование требований к системе защиты информации;
* планирование мероприятий по внутреннему контролю;
* формирование уведомлений в Роскомнадзор;
* формирование согласий на обработку ПДн;
* учет плановых и внеплановых проверок надзорных органов;
* учет сведений о направлении писем в ФСТЭК России;
* ведение журналов по информационной безопасности в электронном виде;
* оценка готовности к проверкам Роскомнадзора;
* оценка готовности к проверкам ФСБ России;
* оценка готовности к проверкам ФСТЭК России;
* планирование событий, постановка задач и контроль их выполнения;
* формирование отчетности по данным организации;
* информационная поддержка пользователя (консультирование).

# Внесение сведений об организации, ее ресурсах и особенностях обработки информации

Функционал внесение сведений об организации, ее ресурсах и особенностях обработки информации должен обеспечивать описания:

* основных реквизитов организации;
* структурных подразделений, должностей и сотрудников организации. Должна поддерживаться возможность выстраивания иерархии структурных подразделений;
* помещений и хранилищ, используемых для обработки и хранения информации;
* бизнес процессов организации;
* программного обеспечения и технических средств;
* внешнего сетевого взаимодействия ИТ-инфраструктуры организации, используемых информационных технологий и взаимодействия ИСПДн, ОКИИ организации с иными системами;
* СЗИ и СКЗИ;
* ИСПДн, ОКИИ;
* ЦОД, используемых для размещения частей ИСПДн, ОКИИ;
* особенностей эксплуатации СКЗИ;
* особенностей функционирования ОКИИ и значений по показателям критериев значимости;
* перечня ответственных лиц.

Программа для ЭВМ должна предусматривать возможность импорта перечня сотрудников и структурных подразделений, помещений, хранилищ, технических средств из файлов форматов xls, xlsx и csv.

При внесении следующих сведений Программа для ЭВМ должна автоматически их просклонять по падежам:

* ФИО сотрудника;
* должность;
* краткое и полное наименования ИСПДн, ОКИИ.

На каждой веб-странице должны быть предусмотрены краткие справочные комментарии, которые позволяют облегчить процесс ввода данных в Программу для ЭВМ. Должны быть предусмотрены информационные справки, которые помогут пользователю внести правильную информацию в поля на веб-странице.

Должен обеспечиваться ввод данных, достаточный для формирования документов, указанный в пункте 4.3.2.5.

В Программе для ЭВМ должна быть доступна возможность определения следующих ответственных лиц:

| **№ п/п** | **Ответственное лицо** | **Доступные форма назначения ответственного** |
| --- | --- | --- |
| 1 | Заместитель руководителя организации, ответственный за обеспечение информационной безопасности | На одного сотрудника |
| 2 | Ответственный за организацию обработки ПДн | На одного сотрудника |
| 3 | Структурное подразделение, осуществляющее функции по обеспечению информационной безопасности | На одно структурное подразделение |
| 4 | Ответственный за обеспечение безопасности ПДн | * На одного сотрудника; * На одно структурное подразделение; * На нескольких сотрудников; * На каждую ИСПДн один сотрудник |
| 5 | Ответственный за планирование и контроль мероприятий по обеспечению информационной безопасности | * На одного сотрудника; * На нескольких сотрудников; * На каждую ЗОКИИ один сотрудник |
| 6 | Ответственный за управление (администрирование) системой защиты информации (подсистемой безопасности) | * На одного сотрудника; * На нескольких сотрудников; * На каждую ЗОКИИ один сотрудник |
| 7 | Ответственные за выявление компьютерных инцидентов и реагирование на них | На одного или нескольких сотрудников |
| 8 | Сотрудники, которым разрешены действия по внесению изменений в конфигурацию систем | На одного или нескольких сотрудников |
| 9 | Сотрудники, имеющие доступ к содержанию электронного журнала сообщений безопасности (назначаются при наличии хотя бы одной ИСПДн с уровнем защищенности ПДн 1 или 2) | На одного или нескольких сотрудников |
| 10 | Должностные лица, с которыми можно осуществлять взаимодействие по вопросам категорирования ОКИИ | * На одного сотрудника; * На каждый ОКИИ один сотрудник |
| 11 | Ответственный за обеспечение безопасности КИИ | На одного сотрудника |
| 12 | Администратор безопасности ЗОКИИ | * На одного сотрудника; * На нескольких сотрудников; * На каждый ЗОКИИ один сотрудник |
| 13 | Ответственный за эксплуатацию средств криптографической защиты | * На одного сотрудника; * На структурное подразделение; * На нескольких сотрудников |
| 14 | Ответственный за организацию и контроль за работой системы видеонаблюдения | На одного сотрудника |
| 15 | Ответственный за организацию режима доступа в контролируемые зоны | * На одного сотрудника; * На структурное подразделение; * На нескольких сотрудников |
| 16 | Ответственный за реализацию мер обеспечения сохранности ПДн, исключающих несанкционированный доступ к материальным носителям ПДн | На одного или нескольких сотрудников |
| 17 | Ответственный за ведение и сохранность журнала посетителей | * На должности |

Должна быть доступна возможность определению следующих комиссий (с указанием председателя, заместителя председателя, секретаря и членов комиссии):

* комиссия по определению уровня защищённости;
* комиссия по уничтожению ПДн;
* комиссия по оценке вреда, который может быть причинён субъектам ПДн;
* комиссия по осуществлению внутреннего контроля соответствия обработки ПДн;
* комиссия по категорированию ОКИИ.

Должны вычисляться автоматически (на основе внесенных в Программу для ЭВМ сведений): уровень защищённости ПДн при их обработке в ИСПДн, категория значимости ОКИИ.

# Описание реализуемых организационных и технических мер по обеспечению безопасности ПДн

Функционал Программы для ЭВМ должен обеспечивать возможность ввода данных о реализуемых организацией отдельных организационных и технических мерах по обеспечению безопасности ПДн.

Функционал Программы для ЭВМ должен обеспечивать возможность описания реализуемых организационных и технических мер в отношении ИСПДн, одним из следующих способов:

* единое описание в отношении всех ИСПДн;
* описание в отношении каждой ИСПДн;
* описание в отношении определенных групп ИСПДн.

Должна быть обеспечена возможность внесения следующей информации:

* о частях ИСПДн, где реализуется идентификация и аутентификация пользователей;
* о реализуемой парольной политике;
* о параметрах реализации следующих мер обеспечения безопасности, реализуемых при управлении доступом:
  + допустимое количество попыток входа (до блокировки учетной записи);
  + время, в течение которого допускаются попытки входа (до блокировки);
  + время блокирования сеанса доступа пользователя после его бездействия (неактивности);
* о параметрах обеспечения доступности, с указанием:
  + объектов, подлежащих резервному копированию, и периодичностью проведения мероприятий по резервному копированию;
* об объектах, подлежащих антивирусной проверке (проверке на наличие вредоносных компьютерных программ (вирусов)), и частоте проведения антивирусной проверки;
* о составе и содержании событий безопасности, подлежащих регистрации в рамках функционирования системы защиты информации;
* о перечне разрешенных входящих и исходящих сетевых потоков;
* о перечне программного обеспечения, разрешенного к использованию в ИСПДн.

Состав и объем вносимой информации должен зависеть от уровней защищенности ПДн.

Введенные данные должны учитываться при формировании документов, представленных в пункте 4.3.2.5.

# Описание ролевой модели системы разграничения доступа

Процесс ввода данных должен происходить в разрезе описанных в Программе для ЭВМ ИСПДн.

Должна быть обеспечена возможность внесения следующей информации:

* + роли (субъект доступа);
  + объекты, в отношении которых осуществляется управление доступом;
  + уровни доступа ролей к объектам доступа;
  + роли сотрудников при доступе к системе.

Сведения о ролевой модели должны быть отражены документе «Приказ о системе разграничения доступа».

# Управление пользовательскими стилями в документации

В Программе для ЭВМ должно быть доступно определение различных настроек оформления документации для следующих типов документов:

* Приказы;
* Политики, положения и акты;
* Технические документы.

Для всех типов документов должны быть доступны для редактирования следующие параметры:

* шрифт;
* размер шрифта;
* междустрочный интервал;
* отступ абзаца;
* поля страниц (верхнее, нижнее, левое, правое).

Для приказов должны быть доступны следующие настройки:

* возможность загрузки шапки приказа;
* форматирование написания слова «приказ» (размер шрифта и начертание);
* форматирование написания номера приказа, даты утверждения документа и населённого пункта (расположение, выравнивание, размер шрифта и начертание);
* форматирование написания заголовка приказа (выравнивание, размер шрифта, межстрочный интервал, интервал до и после заголовка и начертание);
* выбор написания наименования субъекта трудовых правоотношений («сотрудники» или «работники»), упоминаемого в тексте приказа.
* выбор способа написания даты утверждения НПА, упоминаемых в тексте приказа (цифровой или словесно-цифровой);
* расположение (относительно преамбулы) и начертание написание слова «приказываю» начертание;
* интервал до и после основного текста приказа;
* выбор способа написания кавычек в тексте приказа;
* написание слова «Приложение» в тексте приказа (регистр букв и начертание);
* форматирование блока подписи, согласования и подготовки документа (размер шрифта и начертание);
* форматирование написания название приложений (выравнивание, размер шрифта, межстрочный интервал и начертание);
* нумерация приложений к приказу (написание без/с символом «№», выбор вида: арабская, римская, буквенная);
* настройки маркированных списков в приложении (отступ и выбор типа маркера: «-» или «●»);
* форматирование наименования разделов в приложениях (выравнивание, вид нумерации (арабская, римская), начертание, интервал до и после наименования раздела).

Для технических документов должны быть доступны следующие настройки:

* форматирование наименования разделов (выравнивание, вид нумерации (арабская, римская), начертание, интервал до и после наименования раздела);
* выбор способа написания даты утверждения НПА, упоминаемых в тексте приказа (цифровой или словесно-цифровой);
* выбор способа написания кавычек в тексте приказа;
* настройки маркированных списков (отступ и выбор типа маркера: «-» или «●»);
* нумерация приложений к документу (написание без/с символом «№», выбор вида: арабская, римская, буквенная).

Выбранные пользователем настройки оформления должны применяться автоматически при выгрузке документации. Должна быть предусмотрена возможность сохранения нескольких вариантов настроек оформления для всех типов документов.

Должна быть возможность применения на каждый документ типа приказы своего варианта настроек оформления.

Должна быть предусмотрена возможность указания подписанта, согласующих лиц и лиц, подготовивших приказ из числа сотрудников организации.

# Генерация и выгрузка документации

На момент предоставления неисключительных (пользовательских) прав Программа для ЭВМ должна позволять сгенерировать следующие документы:

* Политика в отношении обработки ПДн;
* Приказ об ответственном за организацию обработки ПДн;
* Приказ об ответственном за обеспечение безопасности ПДн;
* Приказ об утверждении перечня сотрудников, имеющих доступ к содержанию электронного журнала сообщений безопасности (в случае, если хотя бы для одной ИСПДн установлен 1 или 2 уровень защищенности ПДн);
* Приказ об утверждении перечня ПДн;
* Приказ об обеспечении безопасности материальных носителей ПДн;
* Приказ о внутреннем контроле соответствия обработки ПДн требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;
* Приказ об утверждении Плана мероприятий по внутреннему контролю режима обработки и защиты ПДн;
* Приказ об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации при ведении журнала учета посетителей;
* Приказ о комиссии по уничтожению ПДн;
* Приказ о введении в эксплуатацию системы видеонаблюдения;
* Порядок хранения, использования и передачи ПДн сотрудников;
* Акт оценки вреда, который может быть причинен субъектам ПДн;
* Акт определения уровня защищенности ПДн (документ формируется на каждую учтенную в Программе для ЭВМ ИСПДн);
* Приказ о комиссии по определению уровня защищенности ПДн;
* Положение по организации и проведению работ по обеспечению безопасности ПДн;
* Приказ об утверждении перечня ИСПДн;
* Приказ о сотрудниках, осуществляющих обработку ПДн и имеющих доступ к обрабатываемым ПДн;
* Приказ об утверждении форм документов, необходимых в целях выполнения требований законодательства Российской Федерации в области защиты информации;
* Приказ об обеспечении безопасности помещений, в которых размещены ИСПДн;
* Приказ о системе разграничения доступа (документ формируется на каждую ИСПДн);
* Приказ о контролируемых зонах;
* Приказ о реализации мер по защите информации;
* Приказ об утверждении перечня ПО, разрешенного к использованию в ИСПДн;
* Приказ о применении единых правил и процедур реализации мер защиты информации (документ формируется в случае, если организацией принято описание реализуемых организационных и технических мерах по защите информации в отношении определенных групп ИСПДн);
* Модель угроз безопасности информации (документ формируется на каждую ИСПДн, ОКИИ);
* Технический паспорт (документ формируется на ИСПДн);
* Техническое задание на создание системы защиты информации (документ формируется для ИСПДн);
* Приказ об утверждении мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты информации;
* Приказ об ответственном за обеспечение информационной безопасности;
* Приказ о структурном подразделении, осуществляющем функции по обеспечению информационной безопасности;
* Приказ об ответственном за планирование и контроль мероприятий по обеспечению информационной безопасности;
* Приказ об ответственном за управление (администрирование) подсистемой безопасности (системой защиты информации);
* Приказ о сотрудниках, которым разрешены действия по внесению изменений в базовую конфигурацию систем (сетей) и их систем защиты (подсистем безопасности);
* Приказ о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них;
* Приказ о силах обеспечения безопасности ОКИИ;
* Приказ об ответственном за обеспечение безопасности КИИ;
* Приказ о назначении администратора безопасности ОКИИ;
* План мероприятий по реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним нормативных правовых актов;
* Приказ об утверждении Положения о комиссии по категорированию ОКИИ;
* Приказ о комиссии по категорированию ОКИИ;
* Приказ об утверждении перечня ОКИИ, подлежащих категорированию (в том числе форма отправки сведений во ФСТЭК России);
* Акт категорирования ОКИИ;
* Форма утверждения перечня объектов КИИ с ФСТЭК России;
* Сведения о результатах присвоения объекту КИИ категории значимости (документ формируется на каждый ОКИИ).

Наименования документов могут быть изменены в процессе их генерации.

Программа для ЭВМ должна предусматривать возможность отметить каждый документ утвержденным с сохранением утвержденных версии документа.

Должно быть предусмотрено отображение информации о состоянии каждого документа, включая наименование документа и его статусы.

В отношении каждого документа должно быть обеспечено отображение:

* событий, информирующих пользователя о возможных изменениях в документе по отношению к его последней сгенерированной версии. При каждой успешной генерации документа события должны сбрасываться. Должно обеспечиваться либо отображение отсутствия событий, либо отображения одного или нескольких следующих событий:
  + изменения в данных – событие, возникающее при изменениях в данных, используемых для формирования комплекта документов;
  + изменения в шаблоне – событие, возникающее при обновлении шаблона документа без пометки о необходимости переутверждения документа;
  + значительные изменения в шаблоне – событие, возникающее при обновлении шаблона документа с пометкой о необходимости переутверждения документа;
  + изменения оформления – событие, возникающее при изменениях параметров, предусмотренных пунктом 4.3.2.4 настоящего Описания услуг и относящихся к данному типу документа;
  + изменения в лицензии – событие, возникающее при изменении клиентской лицензии;
* результата последней генерации – статус с одним из следующих состояний:
  + ошибка генерации – должен устанавливаться при сбоях в процессе генерации документа;
  + недостаточно данных – должен устанавливаться при отсутствии в Программе для ЭВМ данных, необходимых для формирования документа;
  + сформирован – должен устанавливаться при успешной генерации документа.
* состояния выгрузки – статус с одним из следующих состояний:
  + не выгружен – должен устанавливаться, если документ не был скачан из Программы для ЭВМ;
  + выгружен – должен устанавливаться, если документ был хотя бы один раз скачан из Программы для ЭВМ;
* состояния утверждения. Один из следующих статусов:
  + не требуется – должен устанавливаться, если в отношении документа в Программе для ЭВМ не требуется внесение сведений об утверждении;
  + не утвержден – должен устанавливаться, если в отношении документа в Программе для ЭВМ не внесены сведения об утверждении;
  + утвержден – должен устанавливаться, если в отношении документа в Программе для ЭВМ внесены сведения об утверждении.

Для каждого документа должна быть предусмотрена возможность указания произвольных признаков (меток). Должна быть возможность фильтрации документов по добавленным меткам.

Должна быть предусмотрена возможность предварительного просмотра сгенерированных документов.

Должна быть предусмотрена выгрузка сгенерированных документов, как конкретного документа (в формате \*.docx, \*.pdf), так и всех документов одним архивом (в формате \*.zip).

Должна быть доступна возможность загрузки файлов (электронных документов) в Программу для ЭВМ для хранения и последующего использования (скачивания). По каждому загруженному файлу (электронному документу) должна отображаться следующая информация:

* наименование;
* описание;
* состояние;
* источник.

# Выгрузка форм документов

В Программе для ЭВМ должны быть представлены типовые формы следующих документов, разработанные и поддерживаемые в актуальном состоянии разработчиком Программы для ЭВМ и доступные пользователям для скачивания в форматах docx и pdf:

* Разъяснение субъекту ПДн (работнику) юридических последствий отказа предоставить свои ПДн и (или) дать согласие на их обработку;
* Типовая форма согласия субъекта ПДн на обработку ПДн;
* Типовая форма согласия субъекта ПДн на поручение обработки ПДн третьим лицам;
* Типовая форма согласия субъекта ПДн на передачу ПДн третьим лицам;
* Типовая форма согласия на включение ПДн в общедоступные источники;
* Типовая форма согласия субъекта ПДн на обработку ПДн, разрешенных субъектом ПДн для распространения;
* Типовая форма согласия субъекта ПДн на трансграничную передачу ПДн;
* Обязательство о соблюдении конфиденциальности;
* Уведомление о факте обработки ПДн без использования средств автоматизации;
* Форма ознакомления с положениями законодательства РФ о ПДн, локальными актами по вопросам обработки ПДн;
* Журнал учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора);
* Журнал выдачи и приема ключей от помещений;
* Журнал учета выдачи и приема ключей от помещений и хранилищ, в которых хранятся криптосредства, эксплуатационная и техническая документация к ним, ключевые документы;
* Акт на списание и уничтожение материальных носителей защищаемой информации;
* Уведомление о получении ПДн от третьих лиц;
* Уведомление об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн;
* Уведомление о невозможности удаления ПДн;
* Акт об уничтожении ПДн;
* Образец приказа о наделении полномочиями на период плановой выездной проверки;
* Образец приказа о признании утратившими силу документов по защите ПДн;
* Образец описи документов;
* Образец письма об исполнении предписания;
* Пример пункта о конфиденциальности.

# Оценка угроз безопасности информации

Программа для ЭВМ должна предоставлять возможность оценки угроз безопасности информации в соответствии с Методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 5 февраля 2021 г.

Должна обеспечиваться возможность:

* определения негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации (далее – УБИ);
* определения возможных объектов воздействия и видов воздействия на них;
* определения для каждого объекта воздействия интерфейсов, через которые возможно воздействие на него;
* установления зависимости наступления негативных последствий от воздействия на объекты воздействия;
* описания источников УБИ (антропогенных и техногенных). При описании рассматриваемых нарушителей в отношении каждого нарушителя должна обеспечиваться возможность указания:
  + вида нарушителя (условного наименования нарушителя);
  + категории нарушителя;
  + уровня возможности нарушителя;
  + целей реализации УБИ;
  + предположения об отнесении к числу возможных нарушителей или обоснование исключения из числа возможных нарушителей;
* соотнесения целей реализации УБИ возможных нарушителей с негативными последствиями;
* определения объектов воздействия и их интерфейсов, доступных актуальным нарушителям для реализации УБИ;
* определения возможных способов реализации УБИ;
* определения способов реализации УБИ актуальными нарушителями в отношении объектов воздействия;
* просмотра исключенных из перечня возможных УБИ (УБИ, не характерных для системы (сети));
* просмотра возможных УБИ;
* определения характеристик в отношении каждой возможной УБИ, включающее в себя определение:
  + способов реализации;
  + возможных негативных последствий;
  + сценариев реализации.

Процесс ввода данных должен происходить в разрезе описанных в Программе для ЭВМ ИСПДн, ОКИИ.

По введенным данным в Портфеле документов должен формироваться документ «Модель угроз безопасности информации», по структуре, соответствующий рекомендациям, представленным в Методическом документе «Методика оценки угроз безопасности информации», утвержденном ФСТЭК России 5 февраля 2021 г.

В качестве источника данных об УБИ должен использоваться Банк данных угроз ФСТЭК России (<https://bdu.fstec.ru/>).

# Формирование требований к системе защиты информации

Процесс формирования набора мер защиты информации, подлежащих к реализации в ИСПДн, должен быть реализован в следующим образом:

* автоматическое определение базового набора мер защиты информации: для ИСПДн – исходя из определенного уровне защищенности ПДн;
* автоматическое формирование адаптированного базового набора мер защиты информации. Процесс адаптации должен включать исключение мер, непосредственно связанных с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн. Должна быть доступна возможность:
  + просмотра результатов процесса адаптации базового набора мер защиты информации;
  + исключения мер из адаптированного базового набора мер защиты информации с указанием обоснования исключения;
  + включения в адаптированный базовый набор мер защиты информации мер, исключенных Программой для ЭВМ или пользователем, с указанием обоснования включения;
* возможность уточнения адаптированного базового набора мер защиты информации. Уточнение адаптированного базового набора мер защиты информации должно быть предназначено для дополнения адаптированного набора мер защиты информации мерами из Приказа ФСТЭК России от 18 февраля 2013 г. № 21 с целью адекватного блокирования (нейтрализации) всех угроз безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность;
* возможность дополнения адаптированного базового набора мер защиты информации мерами из Приказа ФСТЭК России от 18 февраля 2013 г. № 21 с целью адекватного блокирования (нейтрализации) или снижения вероятности реализации всех угроз безопасности информации, включенных в модель угроз безопасности информации (Процесс уточнения адаптированного базового набора мер защиты информации);
* возможность дополнения уточненного адаптированного базового набора мер защиты информации мерами, установленными в иных НПА в области защиты информации (Процесс дополнения уточненного адаптированного базового набора мер защиты информации);
* возможность замены мер защиты информации на компенсирующие меры защиты информации, с указанием обоснования применения компенсирующих мер.

Процесс ввода данных должен происходить в разрезе описанных в Программе для ЭВМ ИСПДн.

Сформированный набор мер защиты информации, подлежащий к реализации в ИСПДн, должен быт отражен документе «Техническое задании на создание системы защиты информации».

# Планирование мероприятий по внутреннему контролю

Функционал Программы для ЭВМ должен обеспечивать возможность планирования мероприятий по внутреннему контролю соответствия обработки ПДн требованиям к защите ПДн, установленным Федеральным законом от 27.07.2006 № 152-ФЗ, принятыми в соответствии с ним НПА и локальными актами оператора. Должна быть обеспечена возможность:

* формирования справочника мероприятий по внутреннему контролю;
* формирования ежегодного плана проведения мероприятий по внутреннему контролю режима обработки и защиты ПДн;
* выгрузки ежегодного плана проведения мероприятий по внутреннему контролю режима обработки и защиты ПДн и отчета по нему в формате docx;
* хранения информации по результатам выполнения мероприятий (отчетных материалов);
* формирования плана устранения нарушений, выявленных по результатам мероприятий по внутреннему контролю, с возможностью выгрузки плана в формате docx.

# Формирование уведомлений в Роскомнадзор

Программа для ЭВМ должна обеспечивать возможность сформировать на основе внесенных данных следующие уведомления:

* о намерении осуществлять обработку ПДн;
* об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку ПДн;
* о прекращении обработки ПДн;
* об осуществлении трансграничной передачи ПДн.

Все уведомления должны соответствовать требованиям, установленным приказом Роскомнадзора от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных».

Сформированные уведомления (за исключением уведомления об осуществлении трансграничной передачи ПДн) должны быть доступны к выгрузке в форматах docx и pdf.

С целью передачи сформированных уведомлений через портал ПДн (<https://pd.rkn.gov.ru/>) уполномоченного органа по защите прав субъектов ПДн (Роскомнадзора) Программа для ЭВМ иметь в своем составе специализированный модуль (расширение для веб−браузера на базе Chromium), обеспечивающий автоматическую подстановку данных в поля данных формы подачи уведомлений на портале ПДн.

# Формирование согласий на обработку ПДн

Программа для ЭВМ должна обеспечивать возможность формирования для каждой категории субъектов ПДн согласий на:

* обработку ПДн;
* поручение обработки ПДн;
* передачу ПДн;
* обработку ПДн, разрешенных для распространения;
* включение ПДн в общедоступные источники.

Должна быть доступна возможность формирования одной формы согласия (документа), содержащей в себе все виды согласий (за исключением согласия на обработку ПДн, разрешенных для распространения).

Должна быть предусмотрена возможность предварительного просмотра сформированных форм согласий и их выгрузки в формате docx и pdf.

При формировании форм согласий Программа для ЭВМ должна учитывать особенности обработки ПДн в организации, описанные в Программе для ЭВМ.

# Учет плановых и внеплановых проверок надзорных органов

Программа для ЭВМ должна обеспечивать возможность учета проверок надзорных органов (Роскомнадзор, ФСТЭК России, ФСБ России). При описании проверки должна обеспечиваться возможность внести:

* наименование надзорного органа, осуществляющего контроль;
* дату начала проверки и срок проведения проверки;
* цель проверки;
* наименование проверяемого подразделения, филиала, организации;
* причину проверки;
* сведения о наличии замечаний по результатам проверки (нет данных / без замечаний / получены / устранены);
* установленный надзорным органом срок устранения замечаний;
* размер штрафа, выписанного за нарушения, выявленные в ходе проверки;
* отметку о прохождении проверки;
* комментарий в свободной форме;
* файлы (электронные документы) по результатам прохождения проверок.

# Учет сведений о направлении писем в ФСТЭК России

Функционал Программы для ЭВМ должен обеспечивать возможность формирования сопроводительных писем:

* в ФСТЭК России с перечнем ОКИИ, подлежащих категорированию;
* в ФСТЭК России с результатами категорирования ОКИИ.

Должна быть предусмотрена выгрузка сформированных сопроводительных писем в формате docx.

Должна обеспечиваться возможность внести сведения о реквизитах исходящего и входящего сопроводительного письма.

# Ведение журналов по информационной безопасности в электронном виде

Функционал Программы для ЭВМ должен обеспечивать ведение следующих журналов в электронном виде:

* Журнал поэкземплярного учета средств защиты информации;
* Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов;
* Журнал учета обращений субъектов ПДн;
* Лицевые счета пользователей криптосредств;
* Журнал учета хранилищ (сейфов);
* Журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств;
* Журнал учета машинных носителей ПДн;
* Журнал проверок электронных журналов;
* Журнал учета передачи ПДн;
* Журнал периодического тестирования средств защиты информации;
* Журнал обучения пользователей правилам работы с СКЗИ;
* Журнал резервного копирования и восстановления данных;
* Журнал учета ознакомления сотрудников с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, а также информирования и ознакомления сотрудников по вопросам информационной безопасности.

Для каждой записи в журнале должны фиксироваться дата последнего изменения записи и логин пользователя, который произвел эти изменения.

# Оценка готовности к проверкам Роскомнадзора

Функционал Программы для ЭВМ должен обеспечивать возможность оценки готовности к проверке Роскомнадзора в части соблюдения требований Федерального закона от 27.07.2006 г. «О персональных данных». Оценка готовности должна осуществляться в разрезе мероприятий (сформированных и поддерживаемых разработчиком Программы для ЭВМ), которые организация должна выполнять для того, чтобы быть готовой к проверке. Выполнение мероприятий, связанных с разработкой и утверждением приказов и моделей угроз безопасности информации Программа для ЭВМ должна определять автоматически на основе внесенных в Программу для ЭВМ данных. Отметку о выполнении остальных мероприятий пользователь должен устанавливать вручную.

# Оценка готовности к проверкам ФСБ России

Функционал Программы для ЭВМ должен обеспечивать возможность оценки готовности организации к проверке ФСБ России в части выполнения организационных мер по защите информации и требований по эксплуатации криптосредств. Оценка готовности должна осуществляться в разрезе мероприятий (сформированных и поддерживаемых разработчиком Программы для ЭВМ), которые организация должна выполнять для того, чтобы быть готовой к проверке. Выполнение мероприятий, связанных с разработкой и утверждением приказов, моделей угроз безопасности информации Программа для ЭВМ должна определять автоматически на основе внесенных в Программу для ЭВМ данных. Отметку о выполнении остальных мероприятий пользователь должен устанавливать вручную.

# Оценка готовности к проверкам ФСТЭК России

Функционал Программы для ЭВМ должен обеспечивать возможность оценки готовности организации к проверке ФСТЭК России в части выполнения организационных мер по защите информации. Оценка готовности должна осуществляться в разрезе мероприятий (сформированных и поддерживаемых разработчиком Программы для ЭВМ), которые организация должна выполнять для того, чтобы быть готовой к проверке. Выполнение мероприятий, связанных с разработкой и утверждением приказов, моделей угроз безопасности информации Программа для ЭВМ должна определять автоматически на основе внесенных в Программу для ЭВМ данных. Отметку о выполнении остальных мероприятий пользователь должен устанавливать вручную.

# Планирование событий, постановка задач и контроль их выполнения

В Программе для ЭВМ должен быть предусмотрен календарь, в рамках которого пользователь должен иметь возможность внести информацию о предстоящих событиях. Календарь должен иметь следующие формы отображения: год, месяц, неделя, день. При создании события пользователь должен иметь возможность указать:

* название события;
* место;
* дата начала и окончания;
* частоту повтора события (ежедневно, еженедельно, ежемесячно, ежеквартально, ежегодно);
* время, за которое необходимо напомнить (уведомить пользователя) о событии;
* подведомственные (курируемые) организации, которые следует уведомить о событии;
* комментарий в свободной форме к событию.

В Программе для ЭВМ должна быть возможность работы с задачами (создание, изменение, закрытие и удаление). По каждой задаче должна быть доступна возможность указать:

* название задачи и ее описание;
* исполнителей;
* дату исполнения;
* время, за которое необходимо напомнить (уведомить пользователя) о наступлении даты исполнения задачи;
* комментарий в свободной форме к событию.

# Формирование отчетности по данным организации

Программа для ЭВМ должна предоставлять возможность формировать отчеты на основе данных, введенных пользователем в Программу для ЭВМ. Должна быть обеспечена возможность подготовки как минимум следующих отчётов:

* эксплуатируемые ИСПДн, ОКИИ;
* используемые СЗИ;
* сотрудники.

Должна быть предусмотрена выгрузка сформированных отчетов в форматах docx и pdf.

# Информационная поддержка пользователя (консультирование)

В программе для ЭВМ должен быть реализован встроенный механизм ведения диалога со службой поддержки разработчика Программы для ЭВМ (онлайн-консультант).

# На момент передачи неисключительных прав Программа для ЭВМ должна быть включена в Единый реестр российских программ для электронных вычислительных машин и баз данных https://reestr.digital.gov.ru/reestr/.

# **Требования к результатам услуг и гарантийные обязательства**

# На момент подписания Акта приема-передачи прав, указанного в п. 4.1.1, Исполнитель гарантирует Заказчику качественную бесперебойную работу Программы для ЭВМ в соответствии с требованиями, установленными п. 4.3.

# Гарантийный срок на результат оказанных услуг, в рамках которого Исполнитель гарантирует Заказчику качественную бесперебойную работу Программы для ЭВМ без каких–либо функциональных ограничений, должен соответствовать сроку действия предоставленной лицензии, начиная с даты ее активации.

# **Требования к патентной чистоте и лицензионной чистоте использования Заказчиком Программы для ЭВМ**

# При оказании услуг должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.

# **Сроки оказания услуг**

# Начало оказания услуг: с момента подписания Договора.

# Срок оказания услуг: в течение 30 рабочих дней с момента подписания Контракта.

# **Требования по обеспечению режима конфиденциальности**

# В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, перечень которой определен внутренним распорядительным документом Заказчика, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с Законодательством Российской Федерации.

# **Требования к Исполнителю**

# Исполнитель должен обладать необходимым объёмами лицензионных прав и полномочий для предоставления Заказчику неисключительных (пользовательских) прав на использование Программы для ЭВМ. Для подтверждения данного требования Исполнителем предоставляются заверенные копии следующих документов:

* Свидетельство об официальной регистрации Программы для ЭВМ как программы для ЭВМ, выданное в установленном законом порядке Федеральной службой по интеллектуальной собственности, патентам и товарным знакам, в случае если Исполнитель является Правообладателем (Разработчиком) Программы для ЭВМ;
* Лицензионный договор с Правообладателем (Разработчиком) Программы для ЭВМ с полномочиями Исполнителя на передачу третьим лицам неисключительных (пользовательских) прав на использование Программы для ЭВМ в объёме и способами, предусмотренными условиями настоящего Описания услуг, в случае если Исполнитель не является Правообладателем (Разработчиком) Программы для ЭВМ.