**Утверждено:**

 **Директор ЧОУ Православная гимназия**

 **протоиерей Иоанн Моздор**

**«\_\_\_»\_\_\_\_\_\_\_20\_\_\_г.**

**Должностная инструкция лица, ответственного за организацию обработки персональных данных в ЧОУ Православная гимназия**

**1. Общие положения**

Должностная инструкция лица, ответственного за организацию обработки персональных данных в организации (далее - Инструкция), разработана в соответствии с Постановлением Правительства Российской Федерации [от 21.03.2012 № 211](http://itsec2012.ru/postanovlenie-ot-21-marta-2012-g-n-211) «Об утверждении перечня мер, направленных па обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в организации.

Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от [27.07.2006 № 152-ФЗ «О персональных данных»](http://itsec2012.ru/federalnyy-zakon-ot-27-iyulya-2006-g-n-152-fz-o-personalnyh-dannyh), иными нормативными правовыми актами, настоящей Инструкцией, а также иными локальными нормативными актами организации, регламентирующими вопросы обработки персональных данных.

2. Обязанности лица, ответственного за организацию обработки персональных данных в организации

**2.1. Лицо, ответственное за организацию обработки персональных данных в организации обязано:**

осуществлять внутренний контроль за соблюдением работниками организации законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводить до сведения работников организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

**3. Права лица, ответственного за организацию обработки персональныхданных в организации**

3.1. Лицо, ответственное за организацию обработки персональных данных, имеет право:

принимать решения в пределах совей компетенции; требовать от работников организации соблюдения действующего законодательства, а также локальных нормативных актов организации о персональных данных;

контролировать в Службе осуществление мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

взаимодействовать с управлениями и иными структурными подразделениями организации по вопросам обработки персональных данных.

**4. Ответственность лица, ответственного за организацию обработки персональных данных в организации**

4.1. За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о персональных данных лицо, ответственное за организацию обработки персональных данных в организации, несет предусмотренную законодательством Российской Федерации ответственность.

С инструкцией ознакомлен:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_

**Нормативно-правовые акты по информационной безопасности**

Постиндустриальный век явил за собой стремительное развитие многих сфер, в том числе он не обошел и область компьютерных технологий. Если раньше ЭВМ служила неким вспомогательным механизмом для подсчета сложных операций, то сегодня благодаря машинному коду создаются целые системы и комплексы.

Широкий спрос на компьютерную информацию повлиял, прежде всего, на её экономическую значимость, то есть, информацию сегодня можно купить и продать. Как следствие, многие так и норовят получить её незаконным путем. Именно поэтому был создан ряд комплексных мер по устранению утечки данных, которым требуется обеспечение защиты. Такой категории дали термин «**Информационная безопасность**».

Информационная безопасность – это устойчивость и защищенность системы от специального, преднамеренного вмешательства, целью которого служит кража материалов личного пользования. В таком случае владельцу информации будет нанесён вред. В наши дни выделяют три главных принципа, которые должны выполняться при защите систем и комплексов информации:

1. Целостность. **Информационная безопасность** должна обеспечивать сохранение в первозданном виде программный код, базы данных, таблицы и так далее.
2. Конфиденциальность. Пожалуй, один из главных критериев, обеспечивающий открытие доступа лицам, обладающим необходимыми правами для просмотра, а также внесения изменений.
3. Доступность. Этот принцип обеспечивает беспрепятственное и своевременное получение необходимых данных привилегированным пользователям.

При написании и компиляции системы вопрос **информационной безопасности** является первоочередным. Это связано, прежде всего, с риском утечки данных и возможными сбоями и ошибками при намеренных хакерских атаках и случайных обнаружениях дыр в вашем комплексе.

Обеспечение должной защиты системы – вопрос серьёзный и очень затратный. Помимо того, что вам требуется привести в работу средства защиты, ваша задача заключается в поиске специалистов, отвечающих за обнаружение дыр, их устранение и обновление программных комплексов. Помните, что до запуска средств защиты, вы должны проанализировать их работоспособность, быстродействие и устойчивость к атакам.

На начальном этапе можно воспользоваться следующими средствами: использование динамических паролей, определение привилегированных IP-адресов, запуск маскировки сервера в сети *Internet*.

# Сертифицированные средства защиты информации (СЗИ)

Принятие решения о применении тех или иных средств защиты информации производится на основании [анализа актуальности угроз безопасности](http://itsec2012.ru/5-etap-ustranenie-aktualnyh-veroyatnyh-ugroz-bezopasnosti-informacii).

В зависимости от сетевой инфраструктуры и обрабатываемой информации нужно использовать различные средства защиты информации. Чтобы разобраться, что нужно использовать, достаточно руководствоваться несколькими правилами.

На компьютере, на котором ведётся обработка защищаемой информации, практически в любом случае требуется установка средств защиты от несанкционированного доступа.

Если защищаемая информация в процессе обработки передаётся через сегменты сети, находящиеся вне контролируемой зоны, то необходимо использовать криптографические средства защиты.

Если на компьютере ведётся обработка защищаемой информации и он подключен к локальной сети и/или интернету, то на него необходимо установить персональный межсетевой экран. Если в локальной сети ведётся обработка защищаемой информации и она подключена к международной сети интернету, то на него необходимо установить межсетевой экран.

**Алгоритм**

Практически в любой организации, учреждении или на предприятии существуют компьютеры, как правило, объединённые в сеть, на которых обрабатывается какая-либо информация. Специалист по защите информации должен оценить, какая информация обрабатывается, и создать одну или несколько систем защиты информации в соответствии с действующим законодательством, требованиями регулирующих органов (ФСБ и ФСТЭК) и со здравым смыслом.

Создание системы защиты информации мы условно разделили на 5 этапов:

1 этап: Анализ информации, обрабатываемой в организации, составление перечня информации ограниченого распространения.

2 этап: Разработка организационных документов, регламентирующих общие требования по защите информации в организации.

3 этап: Проведение категоризирования и классификации информационных ресурсов.

4 этап: Определение актуальных угроз безопасности.

5 этап: Устранение актуальных (вероятных) угроз безопасности информации.

# 1 этап: Анализ информации, обрабатываемой в организации, составление перечня информации ограниченного распространения

На первом этапе нам необходимо определить какая информация, циркулирующая в организации, подлежит защите. Для  правильного понимания этого вопроса  необходимо ознакомиться с Указом Президента Российской Федерации об утверждении перечня конфиденциального характера [(действующая редакция)](http://itsec2012.ru/perechen-svedeniy-konfidencialnogo-haraktera-v-red-ukaza-prezidenta-rf-ot-23092005-n-1111) и [Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"](http://itsec2012.ru/federalnyy-zakon-ot-27-iyulya-2006-g-n-149-fz-ob-informacii-informacionnyh-tehnologiyah-i-o) .

В соответствии с п.2 ст.9 ФЗ № 149-ФЗ обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Перечень основных видов информации ограниченного распространения с ссылками на федеральные законы РФ представлен в статье [Перечень информации ограниченного распространения](http://itsec2012.ru/perechen-informacii-ogranichennogo-rasprostraneniya).

Наибольшие проблемы возникают с определением служебной тайны в органах государственной власти.

В связи с отсутствием федерального закона о служебной тайне (несмотря на наличие Постановления N 1233) в настоящее время не существует достаточных правовых оснований относить ту или иную информацию к служебной тайне, ограничивая при этом доступ граждан или организаций к информации о деятельности государственных органов и органов местного самоуправления.

В связи с этим имеет смысл пересмотреть отношение к понятию служебной тайны и определить ее так: служебная тайна - это не относящаяся к государственной тайне, полученная государственным органом или органом местного самоуправления информация, доступ к которой ограничен в соответствии с федеральным законом в интересах иных лиц. При таком понимании служебной тайны к ней будут относиться все иные (за исключением государственной тайны) виды информации ограниченного доступа, находящиеся в обладании государственного органа или органа местного самоуправления.

После проведения анализа информации, обрабатываемой в организации, необходимо утвердить Перечень информации ограниченного распространения организации.

# 2 этап:Разработка организационных документов регламентирующих общие требования по защите информации в организации

Вторым этапом в организации работ по защите информации мы считаем разработку организационных документов, регламентирующих общие требования по защите информации в организации.

Вполне возможно, что на момент проведения работ по защите информации в организации уже приняты определеннные меры по защите информации: установлено антивирусное програмное обеспечение на рабочие станции и сервера, регламентирован доступ на территорию организации, организована физическая охрана территории (помещений) и т.д.

Все эти меры Вы сможете учитывать на следующих этапах построения системы защиты информации, только если принятие этих мер строго регламентировано организационными документами, требования которых распространяются в целом на организацию.

Например: если доступ на територию организации осуществляется через пост вневедомственой охраны с проходом через турникет и фиксацией времени входа-выхода сотрудников, пропуск посетителей осуществляется по пропускам при предъявлении документа, удостоверяющего личность, и т.п., но это не регламетировано никаким документом, с которым под роспись  ознакомлены ответственные должностные лица, и не определены мероприятия по контролю соблюдения установленных требований, то говорить о том, что приняты организационные меры, направленные на физическую защиту объекта, мы не можем.

На этом этапе работ нам необходимо:

1. Выявить и упорядочить (при наличии) документы, регламентирующие вопросы, касающиеся защиты информации.

2. С учетом анализа, проведенного на [первом этапе,](http://itsec2012.ru/1-etap-analiz-informacii-obrabatyvaemoy-v-organizacii-sostavlenie-perechnya-informacii)внести корректировки и дополнения (возможно ужесточение требований в сответствии с наличием в организации информации ограниченого распространения).

3. Разработать недостающие документы.

Итак, какими все-таки документами регламентируются общие требования по защите информации в организации? В этом вопросе все сугубо индивидуально и зависит от множества факторов. Приведем основные.

* Положение о пропускном режиме.
* Приказ о назначении ответственного за защиту информации и распределении обязанностей.
* Инструкция о работе в сети интернет и использовании электронной почты организации.
* Инструкция системного администратора.
* Инструкция по антивирусному контролю.
* Инструкция по парольной защите.
* Инструкция пользователя.
* [План обеспечения непрерывной работы и восстановления работоспособности подсистемы.](http://itsec2012.ru/plan-obespecheniya-nepreryvnoy-raboty-i-vosstanovleniya-rabotosposobnosti-podsistemy)
* [Порядок обращения с информацией, подлежащей защите.](http://itsec2012.ru/poryadok-obrascheniya-s-informaciey-podlezhaschey-zaschite)
* [Концепция обеспечения безопасности информации в автоматизированной системе организации.](http://itsec2012.ru/koncepciya-obespecheniya-bezopasnosti-informacii-v-avtomatizirovannoy-sisteme-organizacii)

При разработке документов необходимо помнить: защите подлежит вся информация, циркулирующая в организации, только подход должен быть дифференцированным. Если к информации ограниченного распространения предъявляется, как одно из основных требований, конфиденциальность, то к информации, не подлежащей защите в соответствии с требованиями федерального законодательства, должны предъявляться требования защиты от уничтожения, модифицирования, блокирования и иных неправомерных действий, которые могут нанести ущерб организации.

Вопрос дифференцированного подхода к защите информации подробно расмотрен на 3 этапе - [Проведение категорирования и классификации информационных ресурсо](http://itsec2012.ru/3-etap-provedenie-kategorirovaniya-i-klassifikacii-informacionnyh-resursov)в.

# 3 этап: Проведение категорирования и классификации информационных ресурсов

.На третьем этапе мы непосредственно переходим к категорированию ресурсов. С целью создания нормативно-методической основы для дифференцированного подхода к защите ресурсов и типизации принимаемых организационных мер в организации разрабатывается [Положение об определении требований по защите (о категорировании) ресурсов автоматизированной системы организации](http://itsec2012.ru/polozhenie-ob-opredelenii-trebovaniy-po-zashchite-o-kategorirovanii-resursov-avtomatizirovannoy). (Далее - Положение)

В  разделе Положения 2.1. **Категории конфиденциальности защищаемой информации,** информация, циркулирующая в организации, раделена на 3 категории:

* «**СТРОГО КОНФИДЕНЦИАЛЬНАЯ**» - к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства (коммерческая и банковская тайны, персональные данные и т.д.), а также информация, ограничения на распространение которой введены решениями руководства ОРГАНИЗАЦИИ, разглашение которой может привести к тяжким финансово-экономическим последствиям для Организации вплоть до банкротства (нанесению тяжкого ущерба жизненно важным интересам его клиентов, корреспондентов, партнеров или сотрудников);
* «**КОНФИДЕНЦИАЛЬНАЯ**» - к данной категории относится информация, не отнесенная к категории «СТРОГО КОНФИДЕНЦИАЛЬНАЯ», ограничения на распространение которой вводятся решением руководства Организации в соответствии с предоставленными ему как собственнику (уполномоченному собственником лицу) информации действующим законодательством правами, разглашение которой может привести к значительным убыткам и потере конкурентоспособности ОРГАНИЗАЦИИ (нанесению ощутимого ущерба интересам его клиентов, корреспондентов, партнеров или сотрудников);
* «**ОТКРЫТАЯ**» - к данной категории относится информация, обеспечения конфиденциальности (введения ограничений на распространение) которой не требуется.

Переходя к классификации, необходимо отметить, что классификация информационных систем персональных данных стоит особняком и регламентирована [Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 " Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"](http://itsec2012.ru/postanovlenie-pravitelstva-rf-ot-1-noyabrya-2012-g-n-1119-ob-utverzhdenii-trebovaniy-k-zashchite).

Классификация Государственных информационных систем регламнтируется [Приказом ФСТЭК от 11 февраля 2013 г. №17 "11 февраля 2013 г. N 17 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"](http://itsec2012.ru/prikaz-fstek-ot-11-fevralya-2013-g-no17-11-fevralya-2013-g-n-17-ob-utverzhdenii-trebovaniy-o)

Для автоматизации процесса определения уровня защищенности и определения класса Государственной информационной системмы нами разработаны следующие сервисы:

1.[Расчет уровня защищенности для ИСПДн.](http://itsec2012.ru/raschet-urovnya-zashchishchennosti-dlya-ispdn)

2.[Расчет класса защищенности для ГИС](http://itsec2012.ru/raschet-klassa-zaschischennosti-dlya-is)

Определение мероприятий по защите осуществляется с учетом модели угроз. В свою очередь порядок составления модели угроз указан в [Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных](http://itsec2012.ru/metodika-opredeleniya-aktualnyh-ugroz-bezopasnosti-personalnyh-dannyh) и основывается на [Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных](http://itsec2012.ru/bazovaya-model-ugroz-bezopasnosti-personalnyh-dannyh-pri-ih-obrabotke-v-informacionnyh-sistemah). Также при использовании средств криптографической защиты на основании [Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ РФ 21 февраля 2008 г. N 149/54-144)](http://itsec2012.ru/metodicheskie-rekomendacii-po-obespecheniyu-s-pomoshchyu-kriptosredstv-bezopasnosti-personalnyh) составляется Модель нарушителя.

Классификация информации ограниченого распространения, не содержащей персональных данных, производится на основании [РД "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации"](http://itsec2012.ru/rukovodyashchiy-dokument-avtomatizirovannye-sistemy-zashchita-ot-nesankcionirovannogo-dostupa-k) (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.)

# 4 этап: Определение актуальных угроз безопасности

Необходимо отметить, что определение актуальных угроз безопасности проводится для каждой информационной системы, в которой ведется обработка информации ограниченого распространения.

Для ИСПДн составляется модель угроз. Воспользуемся [примером заполнения модели угроз](http://itsec2012.ru/files/file-010.doc).

Данный вид определения актуальных угроз безопасности может применяться и для определения угроз безопасности систем, в которых ведется обработка других видов информации ограниченого распространения, но можно воспользоваться и другим вариантом, например.

Вприципе, подходы к системетизации угроз, оформлению документов могут быть разные, но перечень угроз будет зависить только от структуры информационной системы.

Структура - распределенная или локальная, имеет подключение к сети или нет и.т.д.

# 5 этап: Устранение актуальных (вероятных) угроз безопасности информации

После определения актуальных угроз для информационной системы эти угрозы, как вы понимаете, необходимо устранить.

Устранение угроз осуществляется двумя способами: организационными и техническими.

Под устранением угроз организационными методами понимается разработка, и (естественно) соблюдение требований документов, регламентирующих как политику безопасности в организации в целом, так и требования по защите информации, обрабатываемой в конкретной системе. В разработке этих документов Вам поможет раздел [Как защитить информацию](http://itsec2012.ru/kak-zashchitit-informaciyu).

В случае невозможности нейтрализации угроз организационными мерами, должны применятся сертифицированные средства защиты информации.

Для выбора сертифицированных средств защиты информации можно ознакомиться с разделом [Сертифицированные средства защиты информации (СЗИ)](http://itsec2012.ru/sertificirovannye-sredstva-zashchity-informacii-szi). В данном разделе находится подборка средств защиты информации с техническими описаниями, действующими сертификатами и руководствами по эксплуатации. Раздел не является рекламой каких либо СЗИ. В нем подобраны сертифицированные средства защиты информации позволяющие обеспечить полный комплекс мероприятий по защите информации и этот выбор основывался исключительно на личном опыте их использования.

**Утверждаю:**

**Директор ЧОУ Православная гимназия**

**\_\_\_\_\_\_\_\_протоиерей Иоанн Моздор**

|  |  |
| --- | --- |
|  |  |

**ПРАВИЛА**

**обработки персональных данных в**

**Частном общеобразовательном учреждении «Православная классическая гимназия во имя святых равноапостольных Кирилла и Мефодия»**

1. **Общие положения**

1.1. Настоящие правила обработки персональных данных (далее – Правила) определяют цели, содержание и порядок обработки персональных данных (далее – ПДн), меры, направленные на защиту ПДн, а также мероприятия, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области ПДн при предоставлении услуг и обеспечения кадрового учета и бухгалтерской деятельности в ЧОУ Православная гимназия.

1.2. Настоящие Правила определяют политику Гимназии как оператора, осуществляющего обработку ПДн, в отношении обработки и защиты ПДн.

1.3. В целях настоящих Правил используются следующие понятия:

- Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники

- Блокирование ПДн – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

- Информационная система персональных данных (далее – ИСПДН) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

- Конфиденциальность ПДн – обязанность оператора и иных лиц, получивших доступ к ПДн, не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом;

- Обезличивание ПДн – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

- Обработка ПДн – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

- Оператор ПДн , самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку ПДн, а также определяющий цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн при предоставлении государственных и муниципальных услуг и обеспечения кадрового учета и бухгалтерской деятельности;

- ПДн – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

- Предоставление ПДн – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

- Распространение ПДн – действия, направленные на раскрытие ПДн неопределенному кругу лиц;

- Уничтожение ПДн – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

1.4. Настоящие Правила разработаны в соответствии:

- Трудовым кодексом Российской Федерации;

- Налоговым кодексом Российской Федерации;

- Кодексом Российской Федерации об административных правонарушениях;

- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральным законом от 27 июля 2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее – Федеральный закон «Об организации предоставления государственных и муниципальных услуг»);

- Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»;

- постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановлением Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.5. Обработка ПДн в ЧОУ православная гимназия осуществляется с соблюдением порядка и условий, предусмотренных настоящими Правилами и законодательством Российской Федерации в области ПДн.

1.6. В ОО ведется обработка ПДн  следующих категорий субъектов ПДн:

- физические лица, обратившиеся в ОО с целью получения образовательных услуг, и их представителей;

- индивидуальные предприниматели (далее – ИП) и физические лица – представители юридических лиц, фигурирующие в договорах, контрактах;

- сотрудники Гимназии.

1. **Условия и порядок обработки ПДн физических лиц в связи с предоставлением государственных и муниципальных услуг**

2.1. Обработка ПДн физических лиц, обратившихся в ОО для получения образовательных услуг (далее – заявители), и их представителей осуществляется в целях организации предоставления услуг, в том числе в электронной форме.

2.2. При организации предоставления государственных и муниципальных услуг заявителям и их представителям, их ПДн могут извлекаться для обработки из следующих документов, представляемых в форме документов на бумажном носителе или в форме электронных документов:

- документы, удостоверяющие личность гражданина Российской Федерации, в том числе военнослужащих, а также документы, удостоверяющие личность иностранного гражданина, лица без гражданства, включая вид на жительство и удостоверение беженца;

- документы воинского учета;

- свидетельства о государственной регистрации актов гражданского состояния;

- документы, подтверждающие регистрацию по месту жительства или по месту пребывания;

- документы о трудовой деятельности, трудовом стаже и заработке гражданина, а также документы, оформленные по результатам расследования несчастного случая на производстве либо профессионального заболевания;

- документы о соответствующем образовании и (или) профессиональной квалификации, об ученых степенях и ученых званиях и документы, связанные с прохождением обучения, выдаваемые организациями, осуществляющими образовательную деятельность;

- справки, заключения и иные документы, выдаваемые организациями, входящими в государственную, муниципальную или частную систему здравоохранения;

- документы Архивного фонда Российской Федерации и другие архивные документы в соответствии с законодательством об архивном деле в Российской Федерации, переданные на постоянное хранение в государственные или муниципальные архивы;

- решения, заключения и разрешения, выдаваемые органами опеки и попечительства в соответствии с законодательством Российской Федерации об опеке и попечительстве;

- удостоверения и документы, подтверждающие право гражданина на получение социальной поддержки, а также документы, выданные федеральными органами исполнительной власти, в которых законодательством предусмотрена военная и приравненная к ней служба, и необходимые для осуществления пенсионного обеспечения лица в целях назначения и перерасчета размера пенсий;

- документы о государственных и ведомственных наградах, государственных премиях и знаках отличия;

2.4. В рамках рассмотрения обращений граждан Российской Федерации, иностранных граждан и лиц без гражданства подлежат обработке следующие ПДн, которые могут содержаться в обращениях:

- фамилия, имя, отчество (последнее при наличии);

- почтовый адрес;

- паспортные данные;

- адрес электронной почты;

- указанный в обращении контактный телефон;

- иные ПДн, указанные в обращении .

2.7. Заявитель при обращении за предоставлением образовательной услуги подтверждает факт получения указанного согласия в форме, предусмотренной законодательством Российской Федерации, в том числе путем представления документа, подтверждающего факт получения указанного согласия, на бумажном носителе или в форме электронного документа.

2.8. Согласие на обработку ПДн заполняется заявителями в соответствии с типовой формой согласия на обработку ПДн:

- согласие на ПДн данных может быть представлено в виде электронного документа, подписанного квалифицированной электронной подписью.

- согласие на обработку ПДн заявителя также может быть подано представителем заявителя, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя заявителя, полномочия данного представителя на дачу согласия от имени заявителя проверяются .

2.9. Обработка ПДн заявителей, необходимых для организации предоставления государственных и муниципальных услуг включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.10.  Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн заявителей для получения образовательной услуги, осуществляется путем:

- получения оригиналов необходимых документов (заявление);

- заверения копий документов;

- внесения сведений в учетные формы (на бумажных и электронных носителях);

- внесения ПДн в прикладное программное обеспечение.

2.11. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн осуществляется путем получения ПДн непосредственно от заявителей или от их законных представителей.

2.12. При организации предоставления услуги запрещается запрашивать у заявителей и третьих лиц ПДн, а также обрабатывать такие ПДн в случаях, не предусмотренных законодательством Российской Федерации.

2.13. При сборе ПДн сотрудники ОО осуществляющие получение ПДн непосредственно от заявителей, обязаны разъяснить указанным заявителям юридические последствия отказа предоставить ПДн.

2.14. Передача (предоставление, доступ) и использование ПДн заявителей осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

1. **Условия и порядок обработки ПДн сотрудников ЧОУ Православная гимназия.**

3.1. ПДн сотрудников ОО обрабатываются в целях обеспечения кадровой и бухгалтерской деятельности , а также в целях обучения и должностного роста, учета результатов исполнения работниками должностных обязанностей, обеспечения им условий труда, гарантий и компенсаций, сохранности принадлежащего им имущества.

3.2. В целях, предусмотренных пунктом 2.1 настоящих Правил, обрабатываются следующие категории ПДн сотрудников ЧОУ Православная гимназия:

- фамилия, имя отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

- серия и номер паспорта, кем и когда выдан;

- информация о гражданстве (в том числе предыдущие гражданства, иные гражданства);

- дата и место рождения;

- адрес прописки и проживания;

- телефонные номера (домашний, рабочий, сотовый);

- состояние в браке;

- ИНН и СНИЛС;

- трудовая деятельность до приема на работу;

- место работы и должность;

- период работы и данные о трудовом договоре;

- номер, серия и дата выдачи трудовой книжки;

- сведения о доходах и заработной плате;

- исполнительные листы;

- лицевые счета;

- сведения о контрагентах;

- сведения о квалификации и переподготовке;

- данные о повышении квалификации;

- наименование образовательного учреждения и документ, подтверждающий образование (номер, дата выдачи, специальность);

- ученая степень и звание;

- сведения о наличии специальных знаний или специальной подготовки;

- данные воинского учета;

- данные о наградах, медалях, поощрениях, почетных званиях;

- постановка на учет в ранние сроки беременности;

- временная нетрудоспособность;

- иные ПДн, необходимые для достижения целей, предусмотренных пунктом 3.1 настоящих Правил.

3.3. Обработка ПДн сотрудников осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 3.1 настоящих Правил, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных», Трудовым кодексом Российской Федерации.

3.4. Обработка специальных категорий ПДн сотрудников может осуществляться в рамках целей, определенных пунктом 3.1 настоящих Правил, в соответствии с подпунктом 2.3. пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации, за исключением случаев получения ПДн сотрудника у третьей стороны, при которых в соответствии с пунктом 3 статьи 86 Трудового кодекса Российской Федерации требуется письменное согласие.

3.5. Обработка ПДн сотрудников осуществляется при условии получения от них письменного согласия на обработку ПДн в следующих случаях:

- при передаче (распространении, предоставлении) их ПДн третьим лицам, кроме случаев, предусмотренных действующим законодательством Российской Федерации;

- при принятии решений, порождающих юридические последствия в отношении сотрудников или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их ПДн.

3.6. В случаях, предусмотренных пунктом 3.5 настоящих Правил, согласие сотрудника на обработку его ПДн оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных». Форма согласия утверждается приказом директора.

3.7. Непосредственная обработка ПДн сотрудников осуществляется специалистами Отдела бухгалтерского учета и отчетности, специалистами Отдела правового, кадрового, информационно-аналитического и организационного обеспечения.

3.8. Обработка ПДн сотрудников включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

3.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПДн сотрудников, осуществляется путем получения ПДн непосредственно от указанных лиц:

- получения оригиналов необходимых документов (заявление, трудовая книжка, иные документы, предоставляемые в Отдел правового, кадрового, информационно-аналитического и организационного обеспечения;

- копирования оригиналов документов;

- внесения сведений в учетные формы (на бумажных и электронных носителях);

- формирования ПДн в ходе кадровой работы;

- внесения ПДн в ИСПДн, используемые Отделом правового, кадрового, информационно-аналитического и организационного обеспечения, а также Отделом бухгалтерского учета и отчетности.

3.10. В случае возникновения необходимости получения ПДн сотрудников, у третьей стороны, следует известить об этом сотрудника заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения ПДн.

3.11. Запрещается получать, обрабатывать и приобщать к личному делу сотрудника ПДн, не предусмотренные пунктом 3.2 настоящих Правил, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

3.12. При сборе ПДн сотрудник Отдела правового, кадрового, информационно-аналитического и организационного обеспечения, осуществляющий сбор (получение) ПДн непосредственно от сотрудников, обязан разъяснить указанным субъектам ПДн юридические последствия отказа предоставить их ПДн.

3.13. Форма разъяснения субъекту ПДн юридических последствий отказа представить свои ПДн в связи с поступлением на работу и ее выполнением в ЧОУ Православная гимназия утверждается приказом директора.

3.14. Передача (распространение, предоставление) и использование ПДн сотрудников осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами

1. **Порядок обработки ПДн субъектов ПДн в ИСПДн**

4.1. Обработка ПДн субъектов ПДн осуществляется в ИСПДн ЧОУ Православная гимназия (далее – АИС ЧОУ Православная гимназия ), ИСПДн «ЧОУ Православная гимназия» .

4.2. АИС ЧОУ Православная гимназия содержит ПДн заявителей, предусмотренные настоящими Правилами, и предназначена для обеспечения деятельности ОО

4.3. ИСПДн и ИСПДн « ЧОУ Православная гимназия» содержат ПДн сотрудников ОО, предусмотренные настоящими Правилами, и предназначены для обеспечения кадровой и бухгалтерской деятельности в ЧОУ Православная гимназия.

4.4. Классификация ИСПДн осуществляется в порядке, установленном законодательством Российской Федерации.

4.5. Сотрудниками, имеющими право осуществлять обработку ПДн в ИСПДн, подписывается «Обязательство о неразглашении информации, содержащей персональные данные», по утвержденной форме.

4.6. Таким сотрудникам предоставляется уникальный логин и пароль для доступа к соответствующей ИСПДн. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями сотрудников.

4.7. Информация с ПДн вносится в базы с ПДн и в другие места хранения информации в электронном виде в ручном режиме, при получении информации на бумажном носителе.

4.8. Обеспечение безопасности ПДн, обрабатываемых в ИСПДн, достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, а также принятия мер по обеспечению безопасности.

1. **Сроки обработки и хранения ПДн**

5.1. ПДн граждан, обратившихся в ЧОУ Православная гимназия лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в ОО до достижения целей обработки.

5.2. Заявления и соответствующие документы настоящих Правил, предоставляемые заявителями на бумажном носителе в связи с организацией предоставления образовательных услуг, хранятся на бумажных носителях до достижения целей обработки.

5.3. ПДн, содержащиеся в приказах по личному составу (о приеме, о переводе, об увольнении, об установлении надбавок о поощрениях и т.д.), подлежат хранению в течение 75 лет.

5.4. Документы, содержащие ПДн сотрудников, в том числе сведения о заработной плате, подлежат хранению 75 лет.

5.5. ПДн при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на разных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

5.6. В ОО обеспечивается раздельное хранение ПДн на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящими Правилами.

5.7. Контроль хранения и использования материальных носителей ПДн, не допускающих несанкционированное использование, уточнение, распространение и уничтожение ПДн, находящихся на этих носителях, осуществляют руководители структурных подразделений, осуществляющих обработку ПДн субъектов ПДн.

5.8. Срок хранения ПДн, внесенных в ИСПДн , указанные в пунктах 4.1, 4.2 и 4.3 настоящих Правил, должен соответствовать сроку хранения бумажных оригиналов.

5.9. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом «О персональных данных».

1. **Порядок уничтожения ПДн при достижении целей обработки или при наступлении иных законных оснований**

6.1. Ответственным за организацию обработки персональных данных в ЧОУ Православная гимназия осуществляется систематический контроль и выделение документов, содержащих ПДн, с истекшими сроками хранения и подлежащих уничтожению.

6.2. Вопрос об уничтожении выделенных документов, содержащих ПДн, рассматривается на заседании комиссии, состав которой утверждается приказом директора.

6.3. По итогам заседания составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел; дела проверяются на их комплектность, акт подписывается председателем и членами комиссии и утверждается директором.

6.4. Уничтожение документов, содержащих ПДн, производится членами комиссии путем сжигания или аппаратного измельчения.

6.5. По окончании процедуры уничтожения Ответственным за организацию обработки персональных данных в ОО составляется соответствующий акт об уничтожении документов, содержащих ПДн.

6.6. Уничтожение ПДн на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление ПДн, или программным удалением необходимой информации принятыми для конкретного типа носителя методами.

1. **Ответственные за организацию обработки ПДн в ЧОУ Православная гимназия**

7.1. Директором назначается Ответственный за организацию обработки персональных данных, который курирует вопросы защиты информации в ОО. В полномочия Ответственного за организацию обработки персональных данных входит:

- принятие правовых, организационных и технических мер для обеспечения защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

- организация внутренних проверок на предмет соблюдения сотрудниками требований законодательства Российской Федерации в области ПДн, в том числе требований к защите ПДн;

- инициирование разработки локальных актов по вопросам обработки ПДн, требований к защите ПДн;

- организация контроля приема и обработки обращений и запросов от субъектов ПДн;

- а случае нарушения в ЧОУ Православная гимназия требований к защите ПДн, принимать необходимые меры по восстановлению нарушенных прав субъектов ПДн.

7.2. Ответственный за организацию обработки ПДн, в соответствии с должностной инструкцией, вправе привлекать к реализации вышеуказанных мер по защите информации иных работников ОО с возложением на них соответствующих обязанностей и закреплением ответственности, а также вправе иметь доступ к информации, касающейся обработки ПДн и включающей:

- цели обработки ПДн;

- категории обрабатываемых ПДн;

- категории субъектов, ПДн которых обрабатываются;

- правовые основания обработки ПДн;

- перечень действий с ПДн, общее описание используемых в ЧОУ Православная гимназия способов обработки ПДн;

- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

- дату начала обработки ПДн;

- срок или условия прекращения обработки ПДн;

- сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

7.3. Непосредственное руководство работами, направленных на обеспечение защиты ПДн, а также контроль проводимых работ обеспечивает Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных, которому могут быть делегированы полномочия, перечисленные в пункте 7.2.

7.4. Ответственного за обеспечение безопасности персональных данных информационных систем персональных данных согласно должностной инструкции участвует в разработке внутренних нормативных документов по защите ПДн.

7.5. Должностные лица, при проведении работ, связанных с обработкой ПДн, руководствуются законодательством Российской Федерации в области ПДн и настоящими Правилами.

7.6. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, а также требований к защите ПДн, установленных Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации.

7.8. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

 **СОГЛАСИЕ**

 **на обработку персональных данных**

Я , \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(фамилия, имя, отчество)*

документ удостоверяющий личность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(вид документа)*

выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(кем и когда)*

зарегистрированный (ая) по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

даю свое согласие \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (*КОМУ указать организацию)*

зарегистрированному по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, на обработку своих персональных данных, на следующих условиях:

1.​ Оператор осуществляет обработку персональных данных Субъекта исключительно в целях \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

2.​ Перечень персональных данных, передаваемых Оператору на обработку:

​ •фамилия, имя, отчество;

​ •дата рождения;

​ •паспортные данные;

​ •контактный телефон (дом., сотовый, рабочий);

​ •фактический адрес проживания;

​ •адрес размещения офиса;

​ •прочие.

1.​ Я даю согласие на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий: обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных), при этом общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 № 152-ФЗ, а также на передачу такой информации третьим лицам, в случаях, установленных нормативными документами вышестоящих органов и законодательством.

 Настоящее согласие действует бессрочно.

 Настоящее согласие может быть отозвано мною в любой момент по соглашению сторон. В случае неправомерного использования предоставленных данных соглашение отзывается письменным заявлением субъекта персональных данных.

2.​  По письменному запросу имею право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст.14 Федерального закона от 27.06.2006 № 152-ФЗ).

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Подпись ФИО*

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Подпись ФИО*