

СОГЛАСОВАНО
Советом Учреждения
Протокол
от 18.06 2019 г.
№ 41

УТВЕРЖДЕНО
Приказом директора
БОУ ДО ВО
«Духовно-просветительский
центр «Северная Фиваида»
от 19.06 2019 г.
№ 953

**ПОЛОЖЕНИЕ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Бюджетного образовательного учреждения дополнительного образования
Вологодской области «Духовно-просветительский центр «Северная Фиваида»
(далее – Учреждение)

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обеспечении безопасности персональных данных при обработке в информационной системе персональных данных (далее – Положение) БОУ ДО ВО «Духовно-просветительский центр «Северная Фиваида» устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

1.2. Положение разработано в соответствии с Федеральным Законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (с последующими изменениями), 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», нормативными документами ФСТЭК и ФСБ России с целью обеспечения защиты прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных.

1.3. Для целей настоящего Положения применяются следующие термины и определения:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа к информационным системам персональных данных — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Конфиденциальность персональных данных — Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных – доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

- разграничение полномочий доступа к данным;
- авторизация, контроль и учет действий с данными (регистрация событий);
- контроль копирования, печати, обмена данными по каналам связи;
- межсетевое экранирование и защита от вирусов;
- учет внешних носителей данных;
- резервное копирование / восстановление данных;
- раздельное хранение носителей данных с резервными копиями;
- контроль доступа в помещения и к компьютерам;
- применение устройств идентификации пользователей для д

II. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Настоящим Положением определяется структура и составляющие безопасности информации в информационной системе персональных данных работников Учреждения, обучающихся и их родителей (законных представителей), а также иных участников образовательного процесса.

2.2. Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных – ИСПДн) достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

2.3. Мероприятия по обеспечению безопасности ПДн формулируются на основании анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

Структура, состав и основные функции системы защиты персональных данных определяются исходя из анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн.

2.4. Система защиты персональных данных включает организационные меры и технические средства защиты информации (в том числе шифровальные

(криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

2.5. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн; на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

2.6. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:

1. определение угроз безопасности ПДн при их обработке, формирование на их основе модели угроз;
2. разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности информационных систем;
3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
4. установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;
5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
7. учет лиц, допущенных к работе с ПДн в информационной системе;
8. контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
10. описание системы защиты персональных данных.

2.7. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

2.8. Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации,

представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;
- угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования.

Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

- обследование и оформление документа о типе актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, определение способов и состава средств защиты информации (СЗИ), разработка технического задания (ТЗ) на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование;
- ввод в эксплуатацию – закупка и установка сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации.

III. ЦЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

- целостности информации;
- доступности обрабатываемой информации для зарегистрированных пользователей;
- конфиденциальности информации.

IV. ОБЪЕКТ ЗАЩИТЫ

Объектом защиты является информационная система персональных данных работников Учреждения, обучающихся, их родителей (законных представителей), и других участников образовательного процесса:

- информационные ресурсы:
- персональные данные работников Учреждения, обучающихся и их родителей (законных представителей) (исходная информация, информационные базы данных);
- инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;
- технические информационные системы и средства Учреждения, в которых обрабатывается, хранится и передается информация ПДн;

- помещения объектов Учреждения, в которых размещаются информационные ресурсы, и обрабатывается конфиденциальная информация;
- технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

Критичными свойствами объекта защиты являются:

1. возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;

2. возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;

3. несанкционированная доступность информации, выражающаяся в возможности:

- непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на носитель или транспортную среду с целью перлюстрации, отчуждения, копирования, изменения, подмены и уничтожения информации;

- прямого или косвенного доступа к оборудованию ИСПДн и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ);

- перехвата речевой информации по акустическим и другим каналам утечки (подслушивание).

4. Субъекты информационных отношений

Субъектами информационных отношений являются:

- Работники (субъекты) – физические лица, состоящие в трудовых и иных гражданско-правовых отношениях с Учреждением-оператором;

- Обучающиеся (субъекты) — физические лица, родители (законные представители) которых состоят в договорных и иных гражданско-правовых отношениях с Учреждением-оператором по вопросам оказания услуг в сфере образования, предусмотренных Уставом.

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;

- достоверности (полноты, точности, адекватности, целостности) информации;

- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);

- своевременного доступа (за приемлемое для них время) к необходимой им информации;

- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;