**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное
образовательное учреждение
высшего образования
**“ВОЛГОГРАДСКИЙ
ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”
(ВолгГТУ)**

# ПРИКАЗ

Волгоград

“ 13 “ марта 20 20 г.

№ 130

Об утверждении Положения об обработке
и защите персональных данных
Волгоградского государственного
технического университета

В целях обеспечения исполнения требований Федерального закона Российской Федерации от 27 июля 2006 года № 152 ФЗ «О персональных данных», а также во исполнение п. 3 приказа ректора университета от 23.12.2019 г. №692 «О единой информационной системе (ЕИС) Волгоградского государственного технического университета»

**ПРИКАЗЫВАЮ:**

1. Утвердить и ввести в действие следующие документы:

- Положение об обработке и защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет» (Приложение №1);

- Политика информационной безопасности при работе с персональными данными в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет» (Приложение №2).

2. Начальнику УНИТ-ВЦ Саяпину М.В. опубликовать указанные документы в подразделе «Персональные данные» раздела «Университет» официального сайта ВолгГТУ (http://www.vstu.ru).

3. Руководителям структурных подразделений ВолгГТУ обеспечить ознакомление подчиненных с указанными документами. В срок до 07 апреля 2020 г. представить в УКиСР ВолгГТУ листы ознакомления (Приложение №3 к приказу).

4. Директорам филиалов ВолГТУ при актуализации аналогичных документов, принять указанные документы университета за основу. После утверждения локальных документов организовать ознакомление с ними сотрудников филиалов.

5. Начальнику общего отдела Антоновой В.А. довести приказ до сведения руководителей структурных подразделений ВолгГТУ и директоров филиалов.

6. Контроль за выполнением требований настоящего приказа возложить на первого проректора Кузьмина С.В.

Ректор университета А.В. Навроцкий

Визы:

Первый проректор

_____С. В. Кузьмин

Начальник УКиСР

_____Р. М. Кувшинов

Начальник УНИТ-ВЦ

_____М. В. Саяпин

Директор ЦИТ ИАиС

_____Д. Б. Панов

Начальник общего отдела

_____В. А. Антонова

Начальник УПиИО

_____Я. В. Волкова

Приложение № 1
к приказу ректора университета
от«13» марта 2020 г. № 130

# ПОЛОЖЕНИЕ
## об обработке и защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет»

| | Наименование подразделения | Фамилия И.О. руководителя | Подпись | Дата |
|---|---|---|---|---|
| Разработано | Начальник УНИТ-ВЦ | Саяпин М.В. | | 06.03.2020 |
| Согласовано | Первый проректор | Кузьмин С.В. | | 11.03.2020 |
| Согласовано | Директор ЦИТ ИАиС | Панов Д.Б. | | 11.03.2020 |
| Согласовано | Начальник УКиСР | Кувшинов Р.М. | | 10.03.2020 |
| Согласовано | Начальник общего отдела | Антонова В.А. | | 10.03.2020 |
| Согласовано | Начальник УПиИО | Волкова Я.В. | | 10.03.2020 |
| Проверено | Начальник ОМКОД | Текин А.В. | | 10.03.2020 |

# СОДЕРЖАНИЕ

**1. Общие положения**

Настоящее Положение об обработке и защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет» (далее по тексту – ВолгГТУ), является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности ВолгГТУ при обработке персональных данных (далее по тексту – ПДн) субъектов персональных данных университета.

Необходимость разработки Положения обусловлена соблюдением требований законодательства РФ при использовании информационных технологий в процессе обработки информации вообще, и персональных данных в частности.

Настоящее Положение определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (далее по тексту – СЗПДн) ВолгГТУ. Положение формулирует основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Положение разработано в соответствии с системным подходом к обеспечению информационной безопасности, который предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

Положение служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ВолгГТУ, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Положение является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ВолгГТУ;

-принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

- координации деятельности структурных подразделений ВолгГТУ при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн ВолгГТУ.

**2. Определения**

В настоящем Положении используются следующие термины и их определения.

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы**– технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с

использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

**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.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**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.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, 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.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

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

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

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

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект) –** лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость –** слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## 3. Обозначения и сокращения

**АРМ** – автоматизированное рабочее место.

**ИСПДн** – информационная система персональных данных.

**НСД** – несанкционированный доступ.

**ПДн** – персональные данные.

**ПО** – программное обеспечение.

**СЗИ** – средства защиты информации.

**СЗПДн** – система (подсистема) защиты персональных данных.

**ТС** –технические средства.

## 4. Нормативные ссылки

Федеральные законодательные акты:

- Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

- Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных" (далее по тексту 152-ФЗ);

- Постановление 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";

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

- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных".

Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

- приказ от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

- приказ от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008 г.

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.08 г.

Приказ ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 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».

## 5. Цели и задачи системы защиты персональных данных

### 5.1. Цели СЗПДн

СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

Безопасность персональных данных 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 иных несанкционированных действий.

Структура, состав и основные функции технических и организационных мероприятий СЗПДн определяются исходя из уровня защищенности (класса) ИСПДн, установленного в соответствии с требованиями Постановления Правительства № 1119 от 1 ноября 2012 г., приказа ФСТЭК России № 17 от 11 февраля 2013 г., приказа ФСТЭК России № 21 от 18 февраля 2013 г., а также в соответствии с требованиями Постановления Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». СЗПДн 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.

Эти меры призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);

- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;

- стадия проектирования (разработки проектов) и реализации мер защиты СЗПДн;

- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия СЗПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы обеспечения безопасности ПДн и разработку и введение в действие документов, предусмотренных Политикой информационной безопасности ИСПДн.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн ВолгГТУ.

### 5.2. Задачи СЗПДн

Для достижения основной цели система безопасности ПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования ИСПДн и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа к информации, циркулирующей в ИСПДн, средствам вычислительной техники ИСПДн; аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

- защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

- защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн;
- оборудование и охрана помещений, где хранятся персональные данные;
- соблюдение порядка хранения персональных данных на бумажных носителях;
- соблюдение порядка хранения ключей от помещений где хранятся ПДн на бумажных носителях;
- соблюдение порядка работы исполнителей с персональными данными на бумажных носителях информации.

**6. Объекты защиты**

В ВолгГТУ производится обработка персональных данных в информационной системе обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется в процессе работы комиссии, по итогам работ которой составляется акт классификации ИСПДн.

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Список персональных данных, подлежащие защите, определен в Перечне персональных данных, подлежащих защите в ИСПДн.

Объекты защиты включают:
- обрабатываемую информацию;
- технологическую информацию;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

**7. Основные принципы построения системы комплексной защиты информации**

Построение системы обеспечения безопасности ПДн ИСПДн ВолгГТУ и ее функционирование должны осуществляться в соответствии со следующими основными принципами:
- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;

- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

**Законность** предполагает осуществление защитных мероприятий и разработку СЗПДн ВолгГТУ в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ИСПДн ВолгГТУ должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение порядка защиты ПДн.

**Системность** - системный подход к построению СЗПДн ВолгГТУ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн ВолгГТУ.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

**Комплексность** - комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

**Непрерывность защиты ПДн.** Защита ПДн – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

**Своевременность -** предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

**Преемственность и совершенствование -** предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

**Персональная ответственность** Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

**Принцип минимизации полномочий –** означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

**Взаимодействие и сотрудничество -** предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн ВолгГТУ, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

**Гибкость системы защиты ПДн.** Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

**Открытость алгоритмов и механизмов защиты.** Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления

(даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

**Простота применения средств защиты.** Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

**Научная обоснованность и техническая реализуемость.** Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

**Специализация и профессионализм.** Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами ВолгГТУ.

**Обязательность контроля.** Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

## 8. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

**Законодательные (правовые) меры защиты.**

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и

использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

**Морально-этические меры защиты.**

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

**Организационные (административные) меры защиты.**

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер – сформировать Политику информационной безопасности ПДн и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне ВолгГТУ в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;
- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также их установить ответственность;
- кто имеет права доступа к ПДн;
- какими мерами и средствами обеспечивается защита ПДн;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;
- определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;
- организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

**Физические меры защиты.**

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

**Аппаратно-программные средства защиты ПДн.**

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн ВолгГТУ;

- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов, изложенных в разделе 7, предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИСПДн ВолгГТУ разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства ВолгГТУ;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);
- специалистами ВолгГТУ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

## 9. Контроль эффективности СЗПДн

Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

## 10. Сферы ответственности за безопасность ПДн

Ответственным за разработку мер контроля за обеспечением безопасности персональных данных является руководство ВолгГТУ. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

Сфера ответственности руководителя включает следующие направления обеспечения безопасности ПДн:

- планирование и реализация мер по обеспечению безопасности ПДн;
- анализ угроз безопасности ПДн;
- разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

Договор, заключенный с соблюдением требований законодательства РФ, между университетом (Заказчиком) и сторонней организацией (Исполнителем), с целью оказания услуг по обработке персональных данных или обслуживанию элементов ИСПДн, должен содержать раздел, определяющий условия обработки конфиденциальной информации Заказчика и меры, предпринимаемые Исполнителем для обеспечения режима конфиденциальности.

## 11. Модель нарушителя безопасности

Под нарушителем безопасности в ВолгГТУ понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн, а также хранятся ПДн на бумажных носителях;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн, а также хранятся ПДн на бумажных носителях.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных.

## 12. Модель угроз безопасности

Для ИСПДн ВолгГТУ выделяются следующие основные категории угроз безопасности персональных данных:

- угрозы от утечки по техническим каналам;
- угрозы несанкционированного доступа к информации;
- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;
- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);
- угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;
- угрозы преднамеренных действий внутренних нарушителей;

- угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в «Модели угроз безопасности персональных данных в ИСПДн».

**13. Механизм реализации Положения**

Реализация Положения должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИСПДн в средствах обеспечения безопасности информации.

**14. Обработка персональных данных без использования средств автоматизации**

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

-не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

-персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

-документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

-дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

Документы (носители информации), содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и/или опечатываемых шкафах (сейфах).

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных,

не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

-при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях должно быть раздельным.

## 15. Процессы обработки персональных данных в ВолгГТУ

Обработка персональных данных субъектов осуществляется в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет» (Россия, 400005, г. Волгоград, проспект им. В.И. Ленина, д. 28.) и в его филиалах:

- Волжский политехнический институт (404121, Россия, Волгоградской обл., г. Волжский, ул. Энгельса, 42а);

-Камышинский технологический институт (403874, Россия, Волгоградская область, г. Камышин, ул. Ленина, 6а);

- Себряковский филиал (403343, Россия, Волгоградская область, г. Михайловка, ул. Мичурина, 21);

- Волжский научно-технический комплекс (404103, Россия, Волгоградская область, г. Волжский, ул. Александрова, 67).

В своей деятельности в отношении обработки персональных данных филиалы университета руководствуются методами и принципами работы головного учреждения, осуществляя необходимые мероприятия в области обработки персональных данных самостоятельно.

Подразделением, ответственным за внедрение, техническую поддержку и развитие информационных систем ВолгГТУ, является «Управление новых информационных технологий – вычислительный центр» (УНИТ-ВЦ) ВолгГТУ. Сотрудники данного подразделения

привлекаются к обеспечению безопасности обработки персональных данных в ИСПДн университета.

**15.1. Классификация пользователей ИСПДн**

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник ВолгГТУ, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн делятся на три основные категории:

- администраторы информационной безопасности;
- администраторы ИСПДн;
- операторы ИСПДн.

**Администраторы информационной безопасности** – это сотрудники ВолгГТУ, которые занимаются настройкой, внедрением и сопровождением систем безопасности. Администратор ИБ обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

**Администраторы ИСПДн**- это сотрудники ВолгГТУ, ответственные за настройку, внедрение и сопровождение ИСПДн. Обеспечивают функционирование подсистемы управления доступом ИСПДн и уполномочены осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

**Операторы ИСПДн** - сотрудники подразделений ВолгГТУ, участвующие в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

- обладает необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ;
- осуществляют непосредственную обработку персональных данных в рамках своих полномочий, определяемых должностной инструкцией, с соблюдений требований настоящего Положения и иных нормативных актов.

**15.2. Категории субъектов персональных данных ВолгГТУ**

Федеральное государственное бюджетное образовательное учреждение высшего

образования «Волгоградский государственный технический университет» осуществляет обработку персональных данных следующий категорий субъектов персональных данных:

- **работники** - лица, находящиеся или находившиеся в трудовых отношениях с ВолгГТУ, а также лица, являющиеся кандидатами на вакантную должность и вступившие с ВолгГТУ в отношения по поводу приема на работу;

- **абитуриенты** – лица, вступившие в отношения с ВолгГТУ с целью поступления в университет для обучения по образовательным программам, реализуемым университетом;

- **обучающиеся** – лица, проходящие обучение по образовательным программам, реализуемым университетом.

- **контрагенты** – лица, чьи сведения обрабатываются с целью исполнения договоров гражданско-правового характера, в том числе родители или иные законные представители абитуриентов и обучающихся.

- **посетители** – лица, вступающие в отношения с ВолгГТУ при посещении вуза.

**15.3. Общие принципы обработки персональных данных в ВолгГТУ**

На все указанные категории субъектов персональных данных распространяются следующие принципы обработки:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- обработке подлежат только персональные данные, которые отвечают целям их обработки;

- содержание и объем обрабатываемых персональных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

- при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. ВолгГТУ должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

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

- обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, в ВолгГТУ не производится, если иное не предусмотрено законодательством;

- защита персональных данных субъектов персональных данных обеспечивается за счет университета;

- субъект персональных данных обязан сообщать ВолгГТУ достоверные персональные данные, состав которых определяется действующим законодательством РФ и локальными нормативно-правовыми актами университета, а также своевременно сообщать об их изменение в установленные сроки;

- ВолгГТУне имеет право принуждать субъектов персональных данных к отказу от своих прав на защиту персональных данных.

**15.4. Условия обработки персональных данных в ВолгГТУ**

Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

- обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 152-ФЗ при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Субъект персональных данных принимает решение о предоставлении его персональных

данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются ВолгГТУ.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных ВолгГТУ вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 152-ФЗ.

ВолгГТУ вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные 152-ФЗ. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению ВолгГТУ, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если ВолгГТУ поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

### 15.5. Конфиденциальность персональных данных

ВолгГТУ не раскрывает третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Лица, признанные виновными в нарушении требований соблюдения конфиденциальности персональных данных привлекаются к дисциплинарной, административной, гражданско-правовую и уголовной ответственности, в порядке предусмотренном законодательством РФ и локальными нормативными актами.

### 15.6. Обработка персональных данных работников ВолгГТУ

Обработка персональных данных работников ВолгГТУ осуществляется в соответствии с

Трудовым кодексом РФ, иными федеральными законами и локальными нормативно-правовыми актами ВолгГТУ.

Источником персональных данные работника является он сам или третьи лица с обязательным письменным предварительным уведомлением работника и получением от него письменного согласия.

Работник должен быть уведомлен о целях сбора информации, источниках ее получения, а также о последствиях отказа от предоставления письменного согласия на сбор информации. При приеме на работу, а также при любых изменениях правил работы с персональными данными работников университета знакомят с действующими документами ВолгГТУ в области обработки персональных данных.

Персональные данные работников обрабатываются следующими структурными подразделениями ВолгГТУ:

- ректорат;
- управление кадров и социального развития (УКиСР);
- бухгалтерия университета;
- финансово-экономическое управление (ФЭУ);
- управление науки и инноваций (УНиИ);
- отдел охраны труда;
- второе управление;
- общий отдел;
- управление правовых и имущественных отношений (УПиИО);
- иными подразделениями университета.

Перечень структурных подразделений и обрабатываемых ими персональных данных приведен в документе «Перечень персональных данных, обрабатываемых ВолгГТУ». Данный документ, утверждается ректором ВолгГТУ и подлежит корректировке при изменения организационной структуры университета и/или процессов обработки персональных данных.

В своей деятельности указанные подразделения руководствуются настоящим Положением и Политикой информационной безопасности при работе с персональными данными ВолгГТУ.

К обработке персональных данных работников допускаются сотрудники ВолгГТУ, прошедшие инструктаж и ознакомленные с ответственностью за разглашение персональных данных, в соответствии с паспортами информационной безопасности подразделений университета, обрабатывающих персональные данные.

Обработка персональных данных работников осуществляется на бумажных носителях и в электронном виде с использованием средств автоматизации.

В соответствии с действующим законодательством РФ персональные данные работников передаются университетом в электронном виде по защищенным каналам связи в виде персонифицированных отчетов утвержденной формы в:

- Пенсионный фонд РФ (формы СЗВ-М, СЗВ-ТД, СЗВ-СТАЖ, АДВ-1, АДВ-2, АДВ-3);
- Фонд социального страхования (форма 4-ФСС);
- Федеральную налоговую службу (форма 6-НДФЛ, 2-НДФЛ, расчёт страховых взносов);

С целью исполнения требований законодательства РФ по обеспечению выплат заработной платы работников бюджетной сферы на электронные карты системы «МИР» университет осуществляет передачу информации о таких выплатах в электронном виде по

защищенным каналам связи в банки, обслуживающие зарплатные счёта работника. Кроме того, университет осуществляет передачу персональных данных работника в банк с целью перевыпуска электронной карты после обращения работника в УКиСР ВолгГТУ. Передача данных также осуществляется по защищенным каналам связи.

С целью реализации требований Федерального закона "О воинской обязанности и военной службе" от 28.03.1998 N 53-ФЗ университет осуществляет передачу персональных данных соответствующих категорий работников в воинские комиссариаты на бумажных носителях.

В соответствии с Постановлением правительства РФ от 10.07.2013 №528 на сайте вуза публикуются персональные данные руководства и профессорско-преподавательского состава университета.

В соответствии с приказом Министерства науки и высшего образования РФ от 16 октября 2018 г. N 766 на сайте университета публикуются сведения о доходах руководства вуза и членов их семей.

В иных случаях персональные данные работников передаются сторонним организациям и лицам по их запросу с указанием целей передачи и реквизитов запрашивающей стороны. Запрос должен быть предоставлен на бумажном носителе или в электронной форме по защищенным каналам связи в рамках соглашения об электронном взаимодействии между ВолгГТУ и адресатом ответа. Соглашение содержит раздел о мерах, принимаемых сторонами для сохранения режима конфиденциальности передаваемой информации. Передача осуществляется с или без согласия субъекта персональных данных в соответствии с действующим законодательством РФ. Ответ предоставляется в письменной форме на фирменном бланке учреждения и отправляется курьерской службой, либо заказным письмом, или в форме электронного документа, направленного по защищенному каналу связи в рамках электронного взаимодействия с адресатом ответа.

После увольнения работника его личное дело передаётся в архив университета и хранится в течении 75 лет. Деятельность архива университета регламентируется Федеральным законом от 22.10.2004 № 125-ФЗ, иными локальными нормативно-правовыми актами. Действие Федерального закона от 08.07.2006 №152-ФЗ «О персональных данных» на деятельность архива ВолгГТУ не распространяется.

### 15.7. Обработка персональных данных абитуриентов ВолгГТУ

Обработка персональных данных абитуриентов ВолгГТУ осуществляется в соответствии с Законом об образовании РФ, приказом Министерства образования и науки Российской Федерации от 14 октября 2015 г. № 1147 «Об утверждении Порядка приема на обучение по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры», иными федеральными законами и локальными нормативно-правовыми актами ВолгГТУ.

Источником персональных данных абитуриента является он сам или лицо, которому абитуриентом предоставлены соответствующие полномочия (далее – доверенное лицо). Доверенное лицо может осуществлять действия, в отношении которых Правилами приема университета установлено, что они выполняются абитуриентом, и которые не требуют личного присутствия абитуриента (в том числе представлять в университет документы, необходимые для поступления, отзывать поданные документы). Доверенное лицо осуществляет указанные

действия при предъявлении выданной абитуриентом и оформленной в установленном порядке доверенности на осуществление соответствующих действий. Абитуриент должен быть уведомлен о целях сбора информации, источниках ее получения, а также о последствиях отказа от предоставления письменного согласия на сбор информации.

Персональные данные абитуриентов обрабатываются следующими структурными подразделениями ВолгГТУ:

- ректорат;
- приёмная комиссия ВолгГТУ;
- отдел аспирантуры, докторантуры ВолГТУ;
- управление правовых и имущественных отношений (УПиИО);
- управление маркетинга образовательных услуг (УМОУ).

В своей деятельности указанные подразделения руководствуются настоящим Положением и Политикой информационной безопасности при работе с персональными данными ВолгГТУ.

К обработке персональных данных абитуриентов допускаются сотрудники ВолгГТУ, прошедшие инструктаж и ознакомленные с ответственностью за разглашение персональных данных, в соответствии с паспортами информационной безопасности подразделений университета, обрабатывающих персональные данные.

Обработка персональных данных абитуриентов осуществляется на бумажных носителях и в электронном виде с использованием средств автоматизации.

Персональные данные абитуриентов передаются в ФИС ГИА и Приема в соответствии с постановлением Правительства Российской Федерации от 31 августа 2013 г. N 755. Передача информации осуществляется по защищенным каналам связи с аттестованных для этих целей АРМ.

В отношении персональных данных абитуриентов с целью обеспечения публичности и прозрачности процесса зачисления действует режим обязательной и безусловной публикации информации о ходе приёмной кампании.

В соответствии с Порядком приема на обучение по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в общедоступных источниках (на сайте вуза и на стендах приёмной комиссии) публикуются списки подавших документы, результаты вступительных испытаний абитуриентов, рейтинговые списки абитуриентов, приказы о зачислении.

Аналогичные меры касаются и абитуриентов, участвующих в конкурсном отборе на обучение по программам подготовки кадров высшей квалификации в аспирантуре ВолгГТУ.

В иных случаях персональные данные абитуриентов передаются сторонним организациям и лицам по их запросу с указанием целей передачи и реквизитов запрашивающей стороны. Запрос должен быть предоставлен на бумажном носителе или в электронной форме по защищенным каналам связи в рамках соглашения об электронном взаимодействии между ВолгГТУ и адресатом ответа. Соглашение содержит раздел о мерах, принимаемых сторонами для сохранения режима конфиденциальности передаваемой информации. Передача осуществляется с или без согласия субъекта персональных данных в соответствии с действующим законодательством РФ. Ответ предоставляется в письменной форме на фирменном бланке учреждения и отправляется курьерской службой, либо заказным письмом, или в форме электронного документа, направленного по защищенному каналу связи в рамках

электронного взаимодействия с адресатом ответа.

В случае успешного зачисления абитуриента его личное дело передаётся в соответствующее структурное подразделение вуза (деканат факультета или УКиСР университета) согласно локальным нормативным актам, где в дальнейшем обрабатывается в соответствии с действующими нормами и регламентами. Личные дела абитуриентов, не зачисленных в число обучающихся, хранятся в приёмной комиссии до окончания приемной кампании, после чего расформировываются и уничтожаются. Не востребованные оригиналы поданных документов передаются на хранение в архив университета, где хранятся до востребования владельцем.

**15.8. Обработка персональных данных обучающихся ВолгГТУ**

Обработка персональных данных обучающихся ВолгГТУ осуществляется в соответствии с Законом об образовании РФ, иными федеральными законами и локальными нормативно-правовыми актами ВолгГТУ.

Источником персональных данные обучающего является он сам или его законные представители. Обучающийся должен быть уведомлен о целях сбора информации, источниках ее получения, а также о последствиях отказа от предоставления письменного согласия на сбор информации.

Персональные данные обучающихся обрабатываются следующими структурными подразделениями ВолгГТУ:

- ректорат;
- управление кадров и социального развития (УКиСР);
- бухгалтерия университета;
- факультеты университета;
- отдел аспирантуры, докторантуры ВолГТУ;
- второе управление;
- управление маркетинга образовательных услуг (УМОУ);
- управление правовых и имущественных отношений (УПиИО);
- отдел содействия занятости студентов и трудоустройства выпускников.

Перечень структурных подразделений и обрабатываемых ими персональных данных приведен в документе «Перечень персональных данных, обрабатываемых ВолгГТУ». Данный документ, утверждается ректором ВолгГТУ и подлежит корректировке при изменения организационной структуры университета и/или процессов обработки персональных данных.

В своей деятельности указанные подразделения руководствуются настоящим Положением и Политикой информационной безопасности при работе с персональными данными ВолгГТУ.

К обработке персональных данных обучающихся допускаются сотрудники ВолгГТУ, прошедшие инструктаж и ознакомленные с ответственностью за разглашение персональных данных, в соответствии с паспортами информационной безопасности подразделений университета, обрабатывающих персональные данные.

Обработка персональных данных обучающихся осуществляется на бумажных носителях и в электронном виде с использованием средств автоматизации.

В соответствии с действующим законодательством РФ персональные данные студентов передаются университетом в электронном виде по защищенным каналам связи в виде

персонифицированных отчетов утвержденной формы в:

- Федеральную налоговую службу (форма 6-НДФЛ, 2-НДФЛ, расчёт страховых взносов);

С целью исполнения требований законодательства РФ по зачислению стипендии и иных видов выплат на электронные карты системы «МИР» обучающихся университета, ВолгГТУ осуществляет передачу информации о таких выплатах в электронном виде по защищенным каналам связи в банки, обслуживающие стипендиальные счёта обучающегося. Кроме того, университет осуществляет передачу персональных данных обучающегося в банк с целью перевыпуска электронной карты после обращения обучающегося в УКиСР ВолгГТУ. Передача данных также осуществляется по защищенным каналам связи.

В целях исполнения требований Постановления Правительства РФ от 26 августа 2013 г. №729 "О федеральной информационной системе "Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении", университет осуществляет обязательную передачу персональных данных обучающихся и выпускников вуза, включая реквизиты выданных документов об образовании. Передача данных осуществляется в утвержденных электронных шаблонах по защищенным каналам связи.

С целью реализации требований Федерального закона "О воинской обязанности и военной службе" от 28.03.1998 N 53-ФЗ университет осуществляет передачу персональных данных обучающихся в воинские комиссариаты на бумажных носителях.

В иных случаях персональные данные обучающихся передаются сторонним организациям и лицам по их запросу с указанием целей передачи и реквизитов запрашивающей стороны. Запрос должен быть предоставлен на бумажном носителе или в электронной форме по защищенным каналам связи в рамках соглашения об электронном взаимодействии между ВолгГТУ и адресатом ответа. Соглашение содержит раздел о мерах, принимаемых сторонами для сохранения режима конфиденциальности передаваемой информации. Передача осуществляется с или без согласия субъекта персональных данных в соответствии с действующим законодательством РФ. Ответ предоставляется в письменной форме на фирменном бланке учреждения и отправляется курьерской службой, либо заказным письмом, или в форме электронного документа, направленного по защищенному каналу связи в рамках электронного взаимодействия с адресатом ответа.

Через год после отчисления личное дело обучающегося передаётся в архив университета и хранится в течении 75 лет. Деятельность архива университета регламентируется Федеральным законом от 22.10.2004 № 125-ФЗ, иными локальными нормативно-правовыми актами. Действие Федерального закона от 08.07.2006 №152-ФЗ «О персональных данных» на деятельность архива ВолгГТУ не распространяется

### 15.9. Обработка персональных данных контрагентов ВолгГТУ

К контрагентам относятся лица, чьи сведения обрабатываются с целью исполнения договоров гражданско-правового характера, в том числе:

- договоров на поставки товаров, выполнение работ, оказание услуг;

- договоров на оказание платных образовательных услуг, стороной которого является обучающийся и/или его родители, осуществляющие платежи по договору;

- договоров на оказание прочих видов услуг, предусмотренных Уставом ВолгГТУ.

Обработка персональных данных контрагентов осуществляется в соответствии с действующим законодательством РФ, и локальными нормативно-правовыми актами ВолгГТУ.

Персональные данные контрагентов обрабатываются следующими структурными подразделениями ВолгГТУ:

- ректорат;
- бухгалтерия университета;
- финансово-экономическое управление (ФЭУ);
- управление науки и инноваций (УНиИ);
- управление правовых и имущественных отношений (УПиИО);
- управление маркетинга образовательных услуг (УМОУ).

Перечень структурных подразделений и обрабатываемых ими персональных данных приведен в документе «Перечень персональных данных, обрабатываемых ВолгГТУ». Данный документ, утверждается ректором ВолгГТУ и подлежит корректировке при изменения организационной структуры университета и/или процессов обработки персональных данных.

В своей деятельности указанные подразделения руководствуются настоящим Положением и Политикой информационной безопасности при работе с персональными данными ВолгГТУ.

К обработке персональных данных контрагентов допускаются сотрудники ВолгГТУ, прошедшие инструктаж и ознакомленные с ответственностью за разглашение персональных данных, в соответствии с паспортами информационной безопасности подразделений университета, обрабатывающих персональные данные.

В иных случаях персональные данные контрагентов передаются сторонним организациям и лицам по их запросу с указанием целей передачи и реквизитов запрашивающей стороны. Запрос должен быть предоставлен на бумажном носителе или в электронной форме по защищенным каналам связи в рамках соглашения об электронном взаимодействии между ВолгГТУ и адресатом ответа. Соглашение содержит раздел о мерах, принимаемых сторонами для сохранения режима конфиденциальности передаваемой информации. Передача осуществляется с или без согласия субъекта персональных данных в соответствии с действующим законодательством РФ. Ответ предоставляется в письменной форме на фирменном бланке учреждения и отправляется курьерской службой, либо заказным письмом, или в форме электронного документа, направленного по защищенному каналу связи в рамках электронного взаимодействия с адресатом ответа.

Договоры, содержащие персональные данные субъектов-контрагентов, хранятся в соответствующих структурных подразделениях университета в соответствии с номенклатурой дел подразделения, определяющей сроки хранения и порядок уничтожения данных документов.

### 15.10. Обработка персональных данных посетителей университета

Обработка персональных данных этой категории субъектов осуществляется отделом охраны, обеспечивающего пропускной режим средствами системы контроля и управления доступом (СКУД) ВолгГТУ.

Указанные подразделения в своей деятельности руководствуются настоящим Положением, Положением о пропускном и внутриобъектовом режиме ВолгГТУ, иными локальными нормативно-правовыми актами.

Данная деятельность осуществляется в целях обеспечения безопасности посетителей университета, включая его сотрудников и обучающихся, антитеррористической защищенности вуза, поддержания порядка и сохранности материальных ценностей.

Основным методом работы является протоколирование фактов посещения вуза с обработкой ФИО посетителя. СКУД ВолгГТУ протоколирует факты посещения, используя цифровые идентификаторы кампусных карт сотрудников и обучающихся ВолгГТУ. Для прочих посетителей университета используется фиксация фактов посещения в соответствующих журналах с указанием ФИО, даты и времени посещения. Журналы посещения хранятся у начальника отдела охраны в течении срока, определенного в номенклатуре дел подразделения, после чего уничтожаются.

К обработке персональных данных посетителей допускаются сотрудники ВолгГТУ, прошедшие инструктаж и ознакомленные с ответственностью за разглашение персональных данных, в соответствии с паспортами информационной безопасности подразделений университета.

К обработке персональных данных посетителей допускаются сотрудники сторонних организаций, прошедших конкурсный отбор на право предоставления университету услуг по обеспечению безопасности. Данные сотрудники допускаются к работам только после прохождения инструктажа и ознакомления с нормативными документами университета, касающихся безопасности и условий обработки персональных данных субъектов. В этом случае ответственность за сохранение конфиденциальности персональных данных субъектов возлагается на стороннюю организацию в рамках соответствующего раздела договора на оказание услуг или дополнительного соглашения к договору.

В иных случаях персональные данные посетителей передаются сторонним организациям и лицам по их запросу с указанием целей передачи и реквизитов запрашивающей стороны. Запрос должен быть предоставлен на бумажном носителе или в электронной форме по защищенным каналам связи в рамках соглашения об электронном взаимодействии между ВолгГТУ и адресатом ответа. Соглашение содержит раздел о мерах, принимаемых сторонами для сохранения режима конфиденциальности передаваемой информации. Передача осуществляется с или без согласия субъекта персональных данных в соответствии с действующим законодательством РФ. Ответ предоставляется в письменной форме на фирменном бланке учреждения и отправляется курьерской службой, либо заказным письмом, или в форме электронного документа, направленного по защищенному каналу связи в рамках электронного взаимодействия с адресатом ответа.

## 16. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

Структурным подразделением университета, ответственным за документооборот и архивирование (общий отдел ВолгГТУ), осуществляется систематический контроль за составом и состоянием номенклатуры дел подразделений ВолгГТУ, осуществляющих обработку персональных данных. В результате этих мероприятий выделяются документы, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

Решение об уничтожении выделенных документов принимается комиссией структурного подразделения с привлечением назначенного ответственного за обеспечение безопасности персональных данных ВолгГТУ и начальника общего отдела. Состав комиссии определяется в паспорте информационной безопасности подразделения, утверждаемом руководством университета.

Уничтожение бумажных документов и электронных носителей, содержащих

персональные данные, осуществляется методом, исключающим возможность восстановления уничтожаемой информации. По окончании процедуры уничтожения составляется соответствующий Акт, подписываемый членами комиссии структурного подразделения и привлеченными должностными лицами.

## 17. Рассмотрение запросов субъектов персональных данных или их представителей

### 17.1. Права субъекта персональных данных на доступ к его персональным данным

Граждане, являющиеся субъектами персональных данных, обрабатываемых в ВолгГТУ (работники, абитуриенты, обучающиеся, контрагенты и прочие лица, вступающие в отношения с ВолгГТУ) или их представители, согласно письменного согласия субъекта ПД, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных в университете;
- правовые основания и цели обработки персональных данных;
- применяемые в университете способы обработки персональных данных;
- наименование и место нахождения оператора персональных данных, сведения о лицах (за исключением сотрудников университета), которые имеют доступ к персональным данным, или которым могут быть раскрыты персональные данные на основании договора с ВолгГТУ или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения в ВолгГТУ;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;
- информацию об осуществленной или предполагаемой трансграничной передаче данных;
- наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению университета, если обработка поручена или будет поручена такой организации или лицу;
- иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

Граждане, являющиеся субъектами персональных данных, обрабатываемых в ВолгГТУ, вправе требовать от университета уточнения их персональных данных, блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

### 17.2. Состав и форма запроса субъекта персональных данных

Сведения, указанные в пункте 17.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю на основании запроса, который должен содержать:

- номер и серию основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

- сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с ВолгГТУ, как с оператором персональных данных (например номер и/или дату заключения договора, информацию о сроках обучения, иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

- подпись субъекта персональных данных или его представителя;

- почтовый адрес субъекта персональных данных или его представителя, для целей информирования о результатах рассмотрения запроса.

Запрос в письменной форме направляется в виде почтового отправления или доставляется субъектом персональных данных или его представителем лично по адресу оператора персональных данных ВолгГТУ - **Россия, 400005, г. Волгоград, проспект им. В.И. Ленина, д. 28, общий отдел**.

Запросы в электронной форме направляются по адресу **doc@vstu.ru.** Приложенные файлы запроса должны быть подписаны ЭЦП субъекта в соответствии с действующим законодательством РФ.

**17.3. Порядок и сроки обработки запросов субъектов персональных данных**

Запросы субъектов персональных данных обрабатываются в соответствии с законодательством РФ в рамках документа «Положение о порядке рассмотрения обращений граждан Российской Федерации» Запросы регистрируются общим отделом университета в журнале обращений граждан и передаются руководству университета для принятия мер к подготовке ответа на запрос.

Университет, являясь оператором персональных данных, предоставляет ответ на запрос субъекту персональных данных **в течение тридцати дней с даты получения запроса**, исключив из него персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

В случае, если сведения, указанные в пункте 17.1. настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными **не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса**, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в ВолгГТУ или направить повторный запрос в целях получения сведений, указанных в пункте 17.1. настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными **до истечения тридцатидневного срока после получения первоначального ответа**, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 17.2. настоящего Положения, должен содержать обоснование направления повторного запроса.

ВолгГТУ вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, изложенным выше. Такой отказ должен быть мотивированным.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

**18. Ответственный за обеспечение безопасности персональных данных ВолгГТУ.**

Ответственный за обеспечение безопасности персональных данных ВолгГТУ назначается приказом ректора университета, из числа сотрудников категории административно-управленческого персонала.

С целью обеспечения эффективного и безусловного исполнения требований закодательства РФ в распределенной структуре ВолгГТУ, приказами директоров филиалов назначаются ответственные за обеспечение безопасности персональных данных в филиалах. Данные лица координируют свою деятельность с ответственным сотрудником головной организации.

Ответственные за обеспечение безопасности персональных данных в ВолгГТУ и филиалах в своей работе руководствуется законодательством Российской Федерации в области персональных данных, Положениями об обработке и защите персональных данных, утвержденными инструкциями и иными локальными актами ВолгГТУ и филиалов.

**18.1. Обязанности ответственных за обеспечение безопасности персональных данных.**

Ответственные за обеспечение безопасности персональных данных обязаны:

- организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в ВолгГТУ и филиалах, от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- осуществлять внутренний контроль за соблюдением сотрудниками университета требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения сотрудников университета положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществлять контроль за приемом и обработкой запросов субъектов персональных данных или их представителей;
- в случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

**18.2. Права ответственных за обеспечение безопасности персональных данных.**

Ответственные за обеспечение безопасности персональных данных вправе:

- иметь доступ к информации, касающейся обработки персональных данных в университете, включающей цели обработки персональных данных, категории обрабатываемых

персональных данных, категории субъектов, персональные данные которых обрабатываются, правовые основания обработки персональных данных, действия с персональными данными, описания мер, предусмотренных статьями 18.1 и 19 152-ФЗ (в том числе сведения о наличии шифровальных криптографических средств и наименования этих средств), дату начала обработки персональных данных, срок или условия прекращения обработки персональных данных, сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки, сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

- инициировать привлечение к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в ВолгГТУ, иных сотрудников университета, с возложением на них соответствующих обязанностей и закреплением ответственности.

Приложение № 2
к приказу ректора университета
от «13» марта 2020 г. № 130

# ПОЛИТИКА
## информационной безопасности при работе с персональными данными в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет»

| | Наименование подразделения | Фамилия И.О. руководителя | Подпись | Дата |
|---|---|---|---|---|
| Разработано | Начальник УНИТ-ВЦ | Саяпин М.В. | | 06.03.20г |
| Согласовано | Первый проректор | Кузьмин С.В. | | 11.03.20г |
| Согласовано | Директор ЦИТ ИАиС | Панов Д.Б. | | 11.03.20 |
| Согласовано | Начальник УКиСР | Кувшинов Р.М. | | 10.03.2020г |
| Согласовано | Начальник общего отдела | Антонова В.А. | | 10.03.2020 |
| Согласовано | Начальник УПиИО | Волкова Я.В. | | 10.03.2020 |
| Проверено | Начальник ОМКОД | Текин А.В. | | 10.03.2020 |

## СОДЕРЖАНИЕ

**1. Общие положения**

Настоящая Политика информационной безопасности (далее – Политика) в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет» (далее по тексту – ВолгГТУ), является официальным документом, разработанным в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в Положении об обработке и защите персональных данных ВолгГТУ.

Целью настоящей Политики, является обеспечение безопасности объектов защиты ВолгГТУ от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональным данным (далее по тексту – УБПДн) ВолгГТУ.

Безопасность персональных данных достигается путем исключения несанкционированного или случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты определятся документом «Перечень персональных данных обрабатываемых в ВолгГТУ», утверждаемым ректором университета.

Состав ИСПДн подлежащих защите определятся документом «Перечень ИСПДн ВолгГТУ», утверждаемым ректором университета.

**2. Определения**

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного

распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

**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.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**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.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, 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.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

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

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

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

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или

философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект) –** лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость –** слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

## 3. Обозначения и сокращения

**АРМ** – автоматизированное рабочее место.

**ИСПДн** – информационная система персональных данных.

**ЛВС** – локальная вычислительная сеть.

**НСД** – несанкционированный доступ.

**ОС** – операционная система.

**ПДн** – персональные данные.

**ПО** – программное обеспечение.

**СЗПДн** – система (подсистема) защиты персональных данных.

**УБПДн** – угрозы безопасности персональных данных.

## 4. Нормативные ссылки

Федеральные законодательные акты:

- Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных

технологиях и о защите информации";

- Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных";
- Постановление 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";
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных".

Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

- приказ от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";
- приказ от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
- базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008 г.
- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.08 г.

Приказ ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 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».

Локальные нормативные акты, утверждаемые ректором университета:

- Положение об обработке и защите персональных данных ВолгГТУ;
- Перечень персональных данных, обрабатываемых в ВолгГТУ;
- Перечень ИСПДн ВолгГТУ;
- Акт классификации информационной системы персональных данных.

## 5. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- отчета об обследовании ИСПДн и результатах проведения внутренней проверки защиты ПДн на бумажных носителях.

- перечня персональных данных, подлежащих защите;
- акта классификации информационной системы персональных данных;
- модели угроз безопасности персональных данных;
- матрицы доступа пользователей к защищаемым информационным ресурсам ИСПДн;
- руководящих документов ФСТЭК России и ФСБ России.

На основе этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн ВолгГТУ. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в документе «План мероприятий по обеспечению защиты персональных данных».

Для ИСПДн составляется список используемых технических средств защиты (далее - Список), а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- Сервера приложений;
- СУБД;
- границы ЛВС;
- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечивать целостность данных;
- производить обнаружений вторжений.

Список используемых технических средств отражается в «План мероприятий по обеспечению защиты персональных данных». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены Ректором ВолгГТУ или лицом, ответственным за обеспечение защиты ПДн.

**6. Требования к составу системы защиты персональных данных**

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;

- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в документе «Акт классификации информационной системы персональных данных».

**6.1. Подсистемы управления доступом, регистрации и учета**

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

**6.2. Подсистема обеспечения целостности и доступности**

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн ВолгГТУ, а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

**6.3. Подсистема антивирусной защиты**

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн ВолгГТУ.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;

- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

**6.4. Подсистема межсетевого экранирования**

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС.

**6.5. Подсистема анализа защищенности**

Подсистема анализа защищенности должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

**6.6. Подсистема обнаружения вторжений**

Подсистема обнаружения вторжений должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

**6.7. Подсистема криптографической защиты**

Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в ИСПДн ВолгГТУ, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

**7. Пользователи ИСПДн**

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник ВолгГТУ, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его должностными обязанностями.

Пользователи ИСПДн делятся на три категории:

- администраторы информационной безопасности;
- администраторы ИСПДн;
- операторы ИСПДн.

**Администраторы информационной безопасности** – это сотрудники ВолгГТУ, которые занимаются настройкой, внедрением и сопровождением систем безопасности. Администратор ИБ обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

**Администраторы ИСПДн**- это сотрудники ВолгГТУ, ответственные за настройку, внедрение и сопровождение ИСПДн. Обеспечивают функционирование подсистемы управления доступом ИСПДн и уполномочены осуществлять предоставление и разграничение доступа конечного пользователя (Оператора ИСПРд) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

**Операторы ИСПДн** - сотрудники подразделений ВолгГТУ, участвующие в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

- обладает необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ;
- осуществляют непосредственную обработку персональных данных в рамках своих полномочий, определяемых должностной инструкцией, с соблюдений требований настоящего

Положения и иных нормативных актов.

**8. Требования к персоналу по обеспечению защиты ПДн**

Все сотрудники ВолгГТУ, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника его непосредственный начальник, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятыми процедурами работы с элементами ИСПДн и СЗПДн.

Сотрудники ВолгГТУ, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же не допускать их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники ВолгГТУ должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники ВолгГТУ должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ВолгГТУ, третьим лицам.

При работе с ПДн в ИСПДн сотрудники ВолгГТУ обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники ВолгГТУ должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция по ведению паспортов информационной безопасности подразделений;
- Инструкция ответственного за обеспечение безопасности персональных данных;
- Инструкция администратора информационной безопасности;
- Инструкция администратора ИСПДн по обеспечению информационной безопасности при обработке персональных данных;
- Инструкция пользователя по обеспечению информационной безопасности при обработке персональных данных в ИСПДн;
- Инструкция по организации парольной защиты;
- Инструкция по организации антивирусной защиты;
- Инструкция по учету и хранению съемных носителей;
- Инструкция по резервированию и восстановлению работоспособности ИСПДн;
- Инструкция по обеспечению безопасности персональных данных при возникновении нештатных ситуаций;
- Инструкция по работе с обезличенными данными;
- Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн;
- Инструкция по уничтожению носителей, содержащих персональные данные;
- Инструкция по предоставлению доступ в ИСПДн ВолгГТУ.

**9. Ответственность сотрудников**

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей.

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Положения о деятельности структурных подразделений ВолгГТУ и должностные инструкции сотрудников университета, осуществляющих обработку ПДн в ИСПДн, должны разрабатываться с учётом требований настоящего документа и содержать информацию об ответственности должностных лиц за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

Приложение №3
к приказу ректора университета
от«13» марта 2020 г. № 130

## Лист ознакомления

Мы, сотрудники подразделения _____,
ознакомлены с документами:

- Положение об обработке и защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет»;

- Политика информационной безопасности при работе с персональными данными в федеральном государственном бюджетном образовательном учреждении высшего образования «Волгоградский государственный технический университет»

| №п/п | ФИО | Должность | Дата | Подпись |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |