Частное образовательное учреждение высшего образования
«ВЯТСКИЙ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЙ ИНСТИТУТ»

«УТВЕРЖДАЮ»
ректор ЧОУ ВО «ВСЭИ»
_____ В.С. Сизов
«10» января 2022 г.

ЧОУ ВО «ВСЭИ»

Сведения о реализуемых требованиях к защите персональных данных в ЧОУ ВО «ВСЭИ»

Защита персональных данных, обрабатываемых ЧОУ ВО «ВСЭИ» (- далее институт) обеспечивается реализацией правовых, организационных и технических мер, необходимых и достаточных для обеспечения требований законодательства в области защиты персональных данных. институт самостоятельно определяет состав и перечень таких мер (ч. 1 ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

1. Правовые меры включают в себя:

- утверждение Политики в отношении обработки персональных данных и размещение ее на интернет-сайте института;
- утверждение иных локальных нормативных актов в области персональных данных;
- назначение лица, ответственного за организацию обработки персональных данных работников и обучающихся;
- назначение лица, ответственного за обеспечение безопасности персональных данных в информационных системах;
- утверждение документа, определяющего перечень работников, имеющих доступ к персональным данным работников и обучающихся и их родителей и (или) законных представителей;
- утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- оформление с работниками, имеющими доступ к персональным данным, обязательств о неразглашении персональных данных;
- заключение с третьими лицами соглашений о неразглашении персональных данных (конфиденциальности).

2. Организационные меры включают в себя:

- размещение технических средств обработки персональных данных в пределах охраняемой территории института;
- обеспечение учета, обращения и хранения материальных носителей персональных данных, исключающих хищение, подмену, несанкционированное копирование, уничтожение персональных данных;
- ограничение допуска посторонних лиц в помещения института, недопущение их нахождения в помещениях, где ведется работа с персональными данными, и

размещаются технические средства их обработки, без контроля со стороны работников института.

- ознакомление работников института, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, с локальными актами института по вопросам обработки персональных данных, и обучение указанных работников;
- определение в трудовых обязанностях и должностных инструкциях работников института обязанностей по обеспечению безопасности обработки персональных данных и ответственности за нарушение установленного порядка;
- определение угроз безопасности персональных данных при их обработке в информационных системах, формирование на их основе моделей угроз;
- для защиты электронных данных обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

3. Технические меры включают в себя:

- определение типа угроз безопасности персональных данных, актуальных для информационных систем персональных данных, с учетом оценки возможного вреда субъектам персональных данных, который может быть причинен в случае нарушения требований безопасности;
- определение уровня защищенности персональных данных при их обработке в информационных системах;
- разработку на основе модели угроз системы защиты персональных данных для уровней защищенности персональных данных при их обработке в информационных системах;
- использование для нейтрализации актуальных угроз средств защиты информации, прошедших процедуру оценки соответствия требованиям Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.
- выявление вредоносного программного обеспечения (применение антивирусных программ) на всех узлах информационной сети института, обеспечивающих соответствующую техническую возможность;
- регулярное резервное копирование информации и баз данных, содержащих персональные данные субъектов персональных данных;
- передача информации с использованием информационно-телекоммуникационных сетей осуществляется при помощи средств криптографической защиты информации.