8 (4212) 47-70-26
e-mail: sputnikgroups@gmail.com | г. Хабаровск, 680000, ул. Пушкина, 54, оф. 507

ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «СПУТНИК» (ЧОУ ДПО «СПУТНИК»)
ИНН 2722980257 / КПП 272101001 / ОГРН 1142700001421

**УТВЕРЖДЕНО**
приказом ЧОУ ДПО «Спутник»

от 31.07.2024 №4/1/07/2024

Генеральным директором
*должность*

/ А.С. Отрешко /
*подпись* *ФИО*

31 июля 2024 года
*дата*

# ПОЛОЖЕНИЕ
# О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ЧОУ ДПО «СПУТНИК»

1. Используемые понятия

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники от внутренних или внешних угроз, при котором обеспечены ее конфиденциальность, доступность и целостность.

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

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

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами, за исключением сведений, составляющих государственную тайну.

Конфиденциальность информации – состояние информации (ресурсов информационной системы), при котором доступ к ней осуществляют только субъекты, имеющие на него право.

Оператор информационной системы (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующий и (или) осуществляющий деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Средства криптографической защиты информации – средства защиты информации, реализующее алгоритмы криптографического преобразования информации.

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

Целостность информации – состояние защищенности информации, характеризуемое способностью обеспечивать сохранность и неизменность защищаемой информации при попытках несанкционированного или случайного воздействия на нее в процессе обработки или хранения.

Общие положения

Настоящее положение о защите информации, обрабатываемой в информационных системах персональных данных ЧОУ ДПО «Спутник» (далее – Положение), разработано на основании:

1) Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных"

Федерального закона Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 №21.

Положение определяет порядок организации и проведения работ по защите информации, обрабатываемой в информационных системах персональных данных (далее - ИСПДн) ЧОУ ДПО «Спутник».

Обладателем информации, содержащейся в ИСПДн является ЧОУ ДПО «Спутник».

Оператором ИСПДн является ЧОУ ДПО «Спутник» (далее – Оператор).

Положение предназначено для Оператора, работников сторонних организаций, допускаемых в установленном порядке к выполнению работ на основных технических средствах и системах ИСПДн по модернизации оборудования и программного обеспечения ИСПДн.

Ответственность за выполнение требований Положения возлагается на Оператора.

Положение вступает в силу с момента его утверждения руководителем ЧОУ ДПО «Спутник» и действует бессрочно, до замены его новым положением.

Тип обрабатываемой информации в ИСПДн

В ИСПДн осуществляется обработка персональных данных и общедоступной информации (общеизвестные сведения и иная информация, доступ к которой не ограничен (ст. 7 Федерального закона №149-ФЗ).

Цели создания системы защиты информации

Целью создания системы защиты информации (далее – СЗИ) в ИСПДн является предотвращение ущерба, возникновение которого возможно в результате утери, хищения, утраты, искажения, подделки информации в любом ее проявлении; реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими законами и нормативными документами по безопасности информации РФ.

Для информации, обрабатываемой в ИСПДн, требуется обеспечить ее конфиденциальность, целостность и доступность.

Основные направления работ по обеспечению безопасности информации

Основными направлениями работ по обеспечению безопасности информации в ИСПДн являются:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;

1) разработка и практическая реализация организационных и технических мероприятий по защите информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) обеспечение возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) осуществление постоянного контроля за обеспечением класса защищенности ИСПДн.

Порядок обработки информации в ИСПДн

Определение необходимого уровня защищенности ИСПДн осуществляется комиссией, сформированной из числа работников ЧОУ ДПО «Спутник». В комиссию должны входить не менее трех человек. По завершении процедуры классификации составляется сответствующий акт.

На этапе проведения процедур классификации ИСПДн комиссией определяется состав информации, подлежащей защите, формируется перечень обрабатываемых ПДн.

Для ИСПДн приказом руководителя ЧОУ ДПО «Спутник» назначается лицо или подразделение, ответственное за организацию защиты информации в ИСПДн – администратор информационной безопасности (далее – Администратор ИБ, АИБ).

Администратора ИБ в своей деятельности руководствуется Инструкцией администратора информационной безопасности.

К техническому обслуживанию средств и систем ИСПДн допускаются только лица, внесенные в списки лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Изменения в конфигурации ИСПДн, влияющие на класс защищенности, должны быть учтены АИБ в соответствующем журнале.

На основные технические средства и системы ИСПДн может устанавливаться только разрешенное к установке лицензионное программное обеспечение.

В ИСПДн все съемные машинные носители и машинные носители информации подлежат учету.

Для определения вероятных нарушителей и актуальных угроз безопасности для ИСПДн разрабатывается модель угроз безопасности ИСПДн.

Ежегодно АИБ разрабатывает план мероприятий по обеспечению защиты информации в ИСПДн на текущий год, который утверждается руководителем ЧОУ ДПО «Спутник».

Администратор ИБ производит учет мероприятий, направленных на обеспечение безопасности информации, обрабатываемой в ИСПДн.

При обработке информации в ИСПДн запрещается:

1) вносить несогласованные изменения в ИСПДн, которые могут снизить класс или уровень защищенности информации;

2) проводить обработку информации без выполнения всех мероприятий по защите информации;

3) допускать к обработке информации лиц, не оформленных в установленном порядке;

4) производить копирование информации на неучтенные носители информации, в том числе для временного хранения информации;

5) обрабатывать информацию на технических средствах в составе ИСПДн при обнаружении каких-либо неисправностей, а также при отключенных средствах защиты информации;

6) обрабатывать защищаемую информацию на технических средствах при окончании сроков действия сертификатов средств защиты информации, за исключением окончания срока действия сертификатов соответствия при условии соблюдения требований по безопасности информации и при наличии действующей технической поддержки на средства защиты информации;

7) передавать информацию за пределы контролируемой зоны без использования средств криптографической защиты.

Ответственность за нарушение норм, регулирующих обработку и защиту информации в ИСПДн

Лицо (подразделение), разрешающее доступ работников к информации, несет персональную ответственность за данное разрешение.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту информации в ИСПДн, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами РФ, а также привлекаются к гражданско-правовой, административной ответственности в порядке, установленном федеральными законами.

Заключительные положения

Администратор ИБ и пользователи ИСПДн обязаны не реже одного раза в 2 года ознакамливаться с Положением.

Администратор ИБ обязан пересматривать и приводить в соответствие положения настоящего документа в случае изменения законодательства Российской Федерации в области защиты информации.