ПРИНЯТО
решением Совета техникума
от «31» августа 2023 г.
Протокол № 3

УТВЕРЖДЕНО
приказом директора техникума
от «01» сентября 2023 г № 1371 о/д

ПОЛОЖЕНИЕ
«Об обеспечении безопасности персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Кропоткинский техникум технологий и железнодорожного транспорта».

1. Определения и сокращения

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

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

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.

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.

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

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.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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

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

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

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

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

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

Угрозы безопасности персональных данных (УБПДн) – 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.

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

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

2. Область применения

2.1. Положение об обеспечении безопасности персональных данных в техникуме (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты ПДн.

2.2. Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности ПДн в техникуме.

2.3. Настоящий документ учитывает положения основных нормативных правовых актов в области защиты ПДн, а именно:

- Федерального закона от 27.07.2006 года № 152-ФЗ “О персональных данных”;
- Постановления Правительства РФ от 17.11.2007 года №781 “Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных”;
- Постановления Правительства РФ от 15.09.2008 года №687 “Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации”;
- Приказа ФСТЭК РФ №55, ФСБ РФ №86, Мининформсвязи РФ №20 от 13.02.2008 года “Об утверждении порядка проведения классификации информационных систем персональных данных”;

2.3.1. Нормативных актов ФСТЭК России:

- “Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных”, утвержденной Заместителем директора ФСТЭК России 15.02.2008 года;
- “Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных”, утвержденной Заместителем директора ФСТЭК России 14.02.2008 года;
- “Положения о методах и способах защиты информации в информационных системах персональных данных”, утвержденного приказам ФСТЭК России от 05.02.2008 года №58;

2.3.2. Нормативных актов ФСБ России:

- “Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных”, утвержденных руководством 8 Центра ФСБ России 21.02.2008 года №149/66-622;

- “Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных с использованием средств автоматизации”, утвержденных руководством 8 Центра ФСБ России 21.02.2008 года №149/54-144.

2.4. Настоящее Положение предназначено для всех сотрудников техникума. Ознакомление с Положением осуществляется под роспись.

2.5. Настоящее Положение вступает в силу с момента его утверждения директором техникума и действует до замены его новым Положением.

2.6. Плановая актуализация Положения проводится не реже, чем два раза в год. Внеплановая актуализация проводится при возникновении следующих условий:

2.6.1. Изменение целей и/или состава обрабатываемых ПДн;

2.6.2. Возникновение условий, существенно влияющих на процессы обработки ПДн и не регламентированных настоящим документом;

2.6.3. По результатам контрольных мероприятий и проверок контролирующих органов исполнительной власти РФ, выявивших несоответствия требованиям по обеспечению безопасности ПДн;

2.6.4. При появлении новых требований к обеспечению безопасности ПДн со стороны российского законодательства и контролирующих органов исполнительной власти РФ.

2.7. Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является ответственный по безопасности ИСПДн.

2.8. Внесение изменений в настоящее Положение производится на основании соответствующего приказа директора техникума.

3. Общие положения

3.1. Техникум является оператором ПДн.

3.2. В техникуме осуществляется обработка ПДн следующих категорий субъектов ПДн: сотрудников техникума, обучающихся в техникуме, данные которых получены техникумом в процессе осуществления своей деятельности.

3.3. Обработка ПДн в техникуме производится с целью и в сроки, указанные в “Положении об обработке персональных данных” и в “Перечне персональных данных”, обрабатываемых в техникуме.

3.4. В техникуме обработка ПДн осуществляется с использованием средств автоматизации и без использования таких средств.

3.5. Сроки хранения ПДн определяются в соответствии со сроком действия договора с субъектом ПДн, а также требованиями законодательства Российской Федерации, устанавливающими сроки хранения документов.

4. Организация работ по обеспечению безопасности персональных данных

4.1. Под организацией работ по обеспечению безопасности ПДн понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредствованного ущерба от реализации УБПДн, и осуществляемых в целях:

- Предотвращения возможных (потенциальных) УБПДн;
- Нейтрализации и/или парирования реализуемых УБПДн;
- Ликвидации последствий реализации УБПДн.

4.2. Организация работ по обеспечению безопасности ПДн в техникуме должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по защите ПДн в техникуме.

4.3. Задачи по приведению техникума в соответствие с требованиями законодательства РФ в области защиты ПДн возлагаются на специалиста, ответственного за информационную безопасность.

4.4. В случаях, когда техникум на основании договора поручает обработку ПДн другому лицу/сторонней организации, необходимо выполнить одно из следующих условий:

- В тексте договора в требованиях к контрагенту прописать обязанность обеспечения контрагентом безопасности и конфиденциальности ПДн;
- В случае невозможности или нецелесообразности изменения текста договора оформить дополнительное соглашение к договору или соглашение о конфиденциальности, в котором прописать обязанность обеспечения контрагентом конфиденциальности и безопасности ПДн при их обработке.

4.5. Работы по приведению техникума в соответствие с требованиями законодательства РФ ведутся по двум направлениям: обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПДн в ИСПДн техникума.

4.6. Работы по обеспечению безопасности ПДн, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- Определение перечня лиц, осуществляющих неавтоматизированную обработку ПДн в техникуме;
- Информирование сотрудников техникума об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;
- Учет и защита носителей ПДн;
- Разграничение доступа к носителям ПДн;
- Уничтожение ПДн.

4.7. Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн техникума, осуществляется в рамках системы защиты персональных данных (далее – СЗПДн), развертываемой в ИСПДн в процессе ее создания или модернизации.

4.8. СЗПДн представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн

информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПДн.

4.9. СЗПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн техникума.

4.10. Для существующих ИСПДн, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПДн, должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.

4.11. Структура, состав и основные функции определяются в соответствии с классом ИСПДн и моделью угроз безопасности ПДн при их обработке в ИСПДн.

5. Проведение работ по обеспечению безопасности персональных данных

5.1. В целях оценки уровня защищенности обрабатываемых в техникуме ПДн и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн в техникуме раз в год должен проводиться анализ изменений процессов защиты ПДн.

5.2. Анализ изменений проводится по следующим направлениям:

- Перечень лиц, участвующих в обработке ПДн, степень их участия в обработке ПДн и характер взаимодействия между собой;
- Перечень и объем обрабатываемых ПДн;
- Цели обработки ПДн;
- Процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения ПДн;
- Способы обработки ПДн (автоматизированная, неавтоматизированная);
- Перечень сторонних организаций, в том числе государственных регулирующих органов, в рамках отношений с которыми осуществляется передача ПДн;
- Перечень программно-технических средств, используемых для обработки ПДн;
- Конфигурация и топология ИСПДн в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- Способы физического подключения и логического взаимодействия компонентов ИСПДн, способы подключения к сетям общего пользования и международного информационного обмена с определением пропускной способности линий связи;
- Режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- Состав используемого комплекса СЗПДн и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн на уровне операционных систем, баз данных и прикладного программного обеспечения;

- Перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн в техникуме;

- Физические меры защиты ПДн.

5.3. Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПДн, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.

5.4. В техникуме должен вестись учет действий, совершаемых с ПДн в ИСПДн сотрудниками техникума.

5.5. Доступ к ПДн регламентируется “Перечнем лиц, допущенных к обработке ПДн”.

5.6. Лица, участвующие в обработке ПДн в техникуме, должны быть проинформированы:

- О факте обработки ими ПДн – реализуется путем ознакомления лиц, обрабатывающих ПДн, с “Перечнем лиц, допущенных к обработке ПДн”;

- О категориях обрабатываемых ПДн – реализуется путем ознакомления с утвержденным “Перечнем персональных данных”;

- О правилах осуществления обработки ПДн – реализуется путем ознакомления под роспись с организационно-распорядительной документацией техникума, регламентирующей процессы обработки ПДн и требованиями законодательства РФ в области ПДн.

5.7. Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ. В техникуме должен вестись учет носителей ПДн.

5.8. Фиксация ПДн должна осуществляться на отдельных материальных носителях (отдельных документах). ПДн должны отделяться от иной информации.

5.9. Фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы ПДн, цели обработки которых несовместимы, должны быть приняты меры по обеспечению раздельной обработки, в частности:

- при необходимости использования или распространения определенных ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн, например, копирование части страницы, содержащей ПДн, которые необходимо использовать, предварительно закрыв остальную часть страницы чистым листом бумаги, либо копирование только необходимых страниц сшитого документа;

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

уничтожению или блокированию, например, копирование только необходимой части страницы, закрыв оставшуюся часть страницы чистым листом бумаги.

5.10. Должен осуществляться мониторинг фактов НСД к ПДн и приниматься соответствующие меры при их обнаружении.

5.11. В техникуме ответственным за безопасность должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности ПДн.

5.12. При обработке ПДн техникум должен иметь возможность и средства для восстановления ПДн при их модификации или уничтожении вследствие НСД.

5.13. Должен быть определен перечень помещений, используемых для обработки ПДн. При этом организация режима безопасности. Охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

5.14. Пользователи ИСПДе должны обеспечивать сохранность съемных носителей, содержащих ПДн. В случае утраты носителя пользователи должны немедленно сообщить об этом администратору безопасности ИСПДн.

5.15. Если при работе с ПДн работнику техникума необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители запираются в отведенных для этого шкафах или сейфах.

5.16. В случае достижения цели обработки ПДн техникум прекращает обработку ПДн и уничтожает ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.17. Проведение работ по созданию (модернизации) СЗПДн техникум включает следующие этапы:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн
- стадия ввода в действие СЗПДн.

5.18. На предпроектной стадии проводится классификация ИСПДн, формируется частная модель угроз безопасности ПДн при их обработке в ИСПДн.

5.19. Классификация ИСПДн осуществляется в соответствии с положениями Приказа ФСТЭК РФ №55, ФСБ РФ №86, Мининформсвязи РФ №20 от 13.02.2008 года “Об утверждении порядка проведения классификации информационных систем персональных данных”.

5.20. Класс ИСПДн оформляется соответствующим актом.

5.21. Частная модель угроз безопасности ПДн при их обработке в ИСПДн формируется на основании руководящих документов ФСТЭК России и ФСБ России.

5.22. Перечень актуальных угроз формируется для каждой ИСПДн техникума с учетом условий функционирования ИСПДн и особенностей обработки ПДн.

5.23. По итогам классификации ИСПДн и результатам определения актуальных УБПДн формируются требования по обеспечению безопасности ПДн, обрабатываемым в ИСПДн.

5.24. Стадия проектирования СЗПДн включает разработку СЗПДн в составе ИСПДн.

5.25. Стадия реализации СЗПДн включает:

- приобретение совокупности используемых в СЗПДн сертифицированных технических, программных и программно-технических средств защиты информации (далее – СЗИ) и их установку;
- определение подразделений и назначение лиц, ответственных за эксплуатацию СЗИ;
- разработку эксплуатационной документации на СЗПДн и СЗИ.

5.26. На стадии ввода в действие СЗПДн осуществляются:

- предварительные испытания СЗИ в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация СЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации.

5.27. В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:

- произошло изменение номенклатуры обрабатываемых ПДн, влекущее за собой изменение класса ИСПДн;
- произошло изменение номенклатуры и/или актуальности УБПДн;
- изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и т.п.).

5.28. Задачи по приведению ИСПДн техникума в соответствие с требованиями законодательства РФ в области защиты ПДн возлагаются на ответственного за безопасность ИСПДн.

5.29. При возникновении условий, влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности ПДн и пр.), необходимо незамедлительно проинформировать об этом ответственного за безопасность ИСПДн.

5.30. Лица, виновные в нарушении требований, предъявляемых законодательством РФ к защите ПДн, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.