Профессиональное образовательное частное учреждение
«Ижевский техникум экономики, управления и права Удмуртпотребсоюза»

«УТВЕРЖДАЮ»

Директор
ПОЧУ «Ижевский техникум экономики,
управления и права Удмуртпотребсоюза»
_____ Е.И. Белова
«30» мая 2019 года

ПОЛОЖЕНИЕ
об обработке и защите персональных данных в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»

г. Ижевск

Определения и принятые 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 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.

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, 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.

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

Система защиты персональных данных (СЗПДн) – совокупность органов и (или) исполнителей, используемая ими техника защиты информации, объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных.

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

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

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

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

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

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

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.

Доступ (доступность) к информации – возможность получения информации и её использования.

Защита информации – деятельность собственника (обладателя, оператора) по обеспечению конфиденциальности, целостности и доступности информации.

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

Несанкционированный доступ (НСД) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим техническим характеристикам и функциональному предназначению.

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

1. Общие положения

1.1. Настоящее положение (далее - Положение) является руководящим документом и определяет содержание и порядок организации работы по обеспечению безопасности персональных данных (далее - ПДн) при их обработке в Профессиональном образовательном частном учреждении «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» (далее – ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»).

1.2. Настоящее Положение принято в целях регулирования работ по защите персональных данных и обеспечения функционирования информационных систем персональных данных ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» в соответствии с требованиями действующего законодательства РФ.

1.3. Положение распространяется на сведения конфиденциального характера, подпадающие под действие утвержденного в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» Перечня персональных данных, которые переданы в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» гражданами на условиях конфиденциальности в целях их обработки в рамках трудовых, и гражданско-правовых отношений.

1.4. Положение является обязательным для выполнения сотрудниками ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», наделенными полномочиями по работе с персональными данными, и предусматривает организационно-правовые и организационно-технические мероприятия, регулирующие порядок, методы и способы защиты персональных данных.

1.5. Требования настоящего Положения являются обязательными для исполнения юридическими и физическими лицами, выполняющими работы в рамках гражданско-правовых отношений.

1.6. Организация и проведение работ по обеспечению безопасности персональных данных проводится на основании законодательных и нормативных актов РФ и уполномоченных органов в области защиты информации, настоящего Положения и нормативно-распорядительных документов ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза».

1.7. Разработка мер по защите информации может осуществляться специализированными организациями на договорной основе, имеющими, если это необходимо, лицензии ФСТЭК и ФСБ РФ на право проведения соответствующих работ.

1.8. Финансирование мероприятий по защите информации предусматривается бюджетом ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» на планируемый год.

1.9. Порядок ввода в действие и изменения Положения.

1.9.1. Настоящее Положение вступает в силу с момента его утверждения директором ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» и действует до замены его новым Положением.

1.9.2. Все изменения и дополнения в Положение вносятся экспертной комиссией и утверждаются приказом директора ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза».

1.10. Режим конфиденциальности персональных данных снимается в случае их обезличивания, признания персональных данных общедоступными, истечения сроков их хранения в соответствии с действующими нормативными документами.

1.11. Все сотрудники ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», имеющие доступ на законном основании к обработке персональных данных, согласно утвержденному директором ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» «Списку допущенных лиц», должны быть ознакомлены с настоящим Положением под роспись.

1.12. Настоящее Положение регламентирует:

- структуру управления процессами построения, функционирования и совершенствования системы защиты персональных данных (далее – СЗПДн);
- порядок определения Перечня персональных данных;
- порядок определения Перечня общедоступных персональных данных;
- порядок определения Перечня носителей персональных данных;
- разрешительную систему допуска и доступа к персональным данным;
-определение уровня защищённости персональных данных при их обработке в информационных системах персональных данных и анализ угроз безопасности персональных данных;
- режимы охраны объектов информатизации;
- инженерно-техническую защиту объектов информатизации;
- программно-аппаратную защиту персональных данных от несанкционированного доступа (далее – НСД);
- криптографическую защиту персональных данных от НСД;
- ролевые функции должностных лиц ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» по защите персональных данных;
- совершенствование и изменение системы защиты персональных данных;

- обязанности и права работников по защите персональных данных;

- обязанности и права оператора по защите персональных данных;

- контроль и надзор за исполнением требований законодательных и нормативных документов;

- ответственность за неисполнение требований законодательных актов.

2. Правовые основы обеспечения безопасности

2.1. Положение разработано в соответствии со следующими законодательными, нормативными и распорядительными документами:

1) Федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ (далее - Закон).

2) Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ.

3) Постановление Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн» (далее - ПП № 1119).

4) Постановление Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации» (далее - ПП № 687).

5) «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн». Утверждена приказом зам. руководителя ФСТЭК РФ 15.02.2008 г.

6) «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн». Утверждена приказом зам. руководителя ФСТЭК РФ 14.02.2008 г.

7) «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн». Утверждено приказом руководителя ФСТЭК РФ от 18.02.2013 г. № 21.

3. Основные требования нормативных документов по защите персональных данных

3.1. К методам и способам защиты персональных данных в информационных системах относятся:

1) Методы и способы защиты персональных данных, обрабатываемых техническими средствами информационной системы, от 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 (далее – методы и способы защиты информации от несанкционированного доступа);

2) Методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий (далее – методы и способы защиты информации от утечки по техническим каналам).

3.2. Для выбора и реализации методов и способов защиты персональных данных в информационной системе, оператором или уполномоченным им лицом, может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

3.3. Для выбора и реализации методов и способов защиты информации в информационной системе может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.4. Выбор и реализация методов и способов защиты персональных данных в информационной системе осуществляются на основе определяемых оператором (уполномоченным лицом) угроз безопасности персональных данных (модели угроз) и в зависимости от уровня защищенности персональных данных при их обработке в информационных системах персональных данных определенного в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных (П.П. № 1119).

3.5. Модель угроз разрабатывается на основе методических документов ФСТЭК России:

1) «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн». Утверждена приказом зам. руководителя ФСТЭК РФ 15.02.2008 г.

2) «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн». Утверждена приказом зам. руководителя ФСТЭК РФ 14.02.2008 г.

3) «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн». Утверждено приказом руководителя ФСТЭК РФ от 18.02.2013 г. № 21.

3.6. Основными методами и способами защиты персональных данных от несанкционированного доступа являются:

1) Реализация разрешительной системы допуска сотрудников ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

2) Ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

3) Разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

4) Регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

5) Учет и хранение съемных носителей информации, и их обращение, исключающее хищение, подмену и уничтожение;

6) Резервирование технических средств, дублирование массивов и носителей информации;

7) Использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

8) Использование защищенных каналов связи;

9) Размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

10) Организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

11) Предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

3.7. Основные мероприятия по защите персональных данных в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»:

3.7.1. Обеспечение безопасности персональных данных в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» путём выполнения комплекса организационно-технических мероприятий по защите персональных данных при их обработке в информационной системе персональных данных.

3.7.2. Обеспечение защиты информации на объектах информатизации ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» путём применения сертифицированных средств защиты информации от попыток несанкционированного доступа и предупреждения, преднамеренных программно-технических воздействий, предпринятых с целью нарушения целостности (модификации, уничтожения) информации в процессе её обработки, передачи, хранения и нарушения её доступности, а также нарушения работоспособности технических средств.

3.8.Порядок определения защищаемой информации ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»:

3.8.1. К защищаемой информации ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» относится:

1) Информация, содержащая персональные данные работников, клиентов, граждан;

2) Общедоступная информация, уничтожение, изменение, блокирование которой может нанести ущерб ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза».

По результатам анализа информации обрабатываемой в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» составляются:

1) Перечень персональных данных;

2) Перечень носителей персональных данных;

3) Описание технологического процесса обработки информации.

3.9.1.Защищаемая информация ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» может быть представлена:

- на бумажных носителях в виде отдельных документов или дел с документами;

- на отчуждаемых и электронных носителях в виде электронных файлов, журналов и баз данных.

3.9.2. С целью определения технических средств, участвующих в обработке персональных данных, администратором безопасности определяются основные технические средства и системы в составе информационной системы персональных данных и их размещение на плане объекта относительно границ контролируемой зоны, утверждённой соответствующим приказом директора ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза».

4. Организация работ по защите персональных данных

4.1 Защита информации, циркулирующей на объекте информатизации, должна быть комплексной и дифференцированной. С этой целью для каждого объекта информатизации создается система защиты информации.

4.2 Защита персональных данных субъектов от неправомерного их использования или утраты обеспечивается в порядке, установленном законодательством РФ.

4.3 Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность в процессе управленческой и иной деятельности организации.

4.4 Защите подлежат:

- информация о персональных данных;
- документы, содержащие персональные данные;
- персональные данные, содержащиеся на материальных, электронных носителях.

4.5 Обеспечение безопасности персональных данных, обрабатываемых в информационной системе персональных данных ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», должно осуществляться на основе следующих принципов:

1) Подконтрольность руководства – деятельность по обеспечению безопасности персональных данных инициируется и контролируется директором ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» и назначенными уполномоченными и ответственными лицами;

2) Соответствие мер и средств защиты актуальным угрозам безопасности персональных данных – проектирование, построение и модернизация системы защиты персональных данных в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» производится на основе анализа угроз безопасности персональных данных и с учетом особенностей эксплуатации информационных систем персональных данных;

3) Комплексность – для защиты персональных данных используется совокупность организационных мер и технических средств защиты;

4) Мониторинг и модернизация – в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» осуществляется регулярный контроль выполнения требований по обеспечению безопасности персональных данных, эффективности применяемых мер и средств защиты, а также уровня защищенности информационной системы персональных данных. На основании анализа результатов контроля планируются и реализуются меры по устранению выявленных недостатков, а также модернизации (совершенствованию) системы защиты персональных данных.

5. Основные мероприятия по защите персональных данных

5.1. В ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» осуществляется защита персональных данных от несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

5.2. Защита персональных данных от несанкционированного доступа включает в себя:

- организационные мероприятия;

- технические мероприятия;
- меры физической защиты.

5.3. Основные организационные мероприятия:

- определение перечня персональных данных, обрабатываемых в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»;
- определение материальных носителей персональных данных;
- анализ актуальности угроз безопасности персональных данных и составление модели угроз безопасности персональных данных;
- организация разрешительной системы и учета носителей, содержащих персональные данные, и лиц, получивших доступ к персональным данным субъектов;
- организация защищенного документооборота (порядка обращения с персональными данными);
- избирательное и обоснованное распределение документов и информации между сотрудниками ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»;
- организация обучения сотрудников ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» по обеспечению безопасной обработки персональных данных;
- регламентация порядка уничтожения носителей, содержащих персональные данные;
- организация контрольно-пропускного режима;
- организация внутриобъектового режима;
- организация контроля выполнения требований по защите персональных данных;
- регулирование отношений по использованию информации, составляющей персональные данные, на правовой основе;
- создание сотрудникам ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» необходимых условий для работы с информацией, составляющей персональные данные.

5.4. Основные технические мероприятия:

- мониторинг и регистрация действий пользователей и обслуживающего персонала в информационной системе;
- резервирование технических средств, дублирование массивов и носителей информации;
- применение межсетевого экранирования;
- применение сканеров безопасности;
- применение систем обнаружения вторжений;
- применение антивирусного программного обеспечения.

5.5. Основные меры физической защиты:

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом директора ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» устанавливается контролируемая зона ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», где определены помещения с ограниченным доступом. Лица, не имеющие доступа к персональным данным, в том числе обслуживающий персонал, а также представители сторонних организаций, при необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных.

5.6. Порядок конкретных мероприятий по защите персональных данных определяется приказами директора ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», иными локальными нормативными документами.

6. Определение перечня персональных данных, обрабатываемых в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»

6.1. Перечень представляет собой список типовой и конкретной информации, попадающей под определение персональных данных.

6.2.Перечень является многоцелевым документом и предназначен для:

- юридического закрепления состава персональных данных, которые могут обрабатываться в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»;

- определения категорий субъектов, чьи персональные данные обрабатываются в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»;

- определения сроков или условий хранения сведений, составляющих персональные данные;

- определения носителей персональных данных;

- определения оснований для обработки персональных данных, а также оснований для прекращения их обработки.

6.3. Перечень персональных данных, обрабатываемых в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», разрабатывается на основании предложений структурных подразделений в пределах своей компетенции, исходя из

документов, содержащих персональные данные, которые используются сотрудниками подразделений в работе.

6.4. Перечень утверждается директором ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» и вводится в действие его приказом.

6.5. Осуществлять обработку и хранение персональных данных, не внесенных в общий Перечень, запрещается.

6.6. Действующий Перечень регулярно (не реже одного раза в год) пересматривается, с целью добавления в него сведений, составляющих персональные данные, или исключения тех персональных данных, обработка которых перестала осуществляться.

6.7. При реорганизации учреждения (в форме слияния, присоединения, разделения, выделения или преобразования) право на установление, изменение или отмену режима конфиденциальности в отношении персональных данных субъектов персональных данных переходит к его правопреемнику.

6.8. При ликвидации учреждения ликвидационная комиссия принимает решение о порядке обработки персональных данных.

7. Определение материальных носителей персональных данных

7.1 Защита сведений, включенных в Перечень персональных данных, осуществляется путем защиты носителей этих сведений.

7.2 Для этого каждый пункт Перечня структурируется на материальные носители сведений, и определяются места расположения этих носителей.

7.3 Создается Перечень материальных носителей персональных данных и схема их расположения.

8. Анализ актуальности угроз безопасности персональных данных

8.1. С целью определения необходимых мер и средств защиты, соответствующих актуальным угрозам безопасности персональных данных при их обработке в информационных системах персональных данных, проводятся анализ и оценка угроз безопасности персональных данных, по результатам которых определяются актуальные угрозы безопасности персональных данных.

8.2. С учетом специфики обработки и обеспечения безопасности персональных данных в информационной системе персональных данных ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» угрозы утечки персональных данных по техническим каналам являются неактуальными.

8.3. На основании результатов проведенного анализа угроз безопасности персональных данных формируется Модель угроз безопасности персональных данных, содержащая следующие сведения:

- перечни характерных для информационной системы угроз безопасности персональных данных, возможных источников угроз и объектов воздействия;
- свойства безопасности информации, нарушаемые при реализации угроз безопасности;
- результаты анализа и оценки ущерба для субъектов персональных данных от реализации угроз безопасности персональных данных;
- результаты анализа и оценки актуальности угроз безопасности персональных данных.

9. Организация контроля выполнения требований по защите персональных данных

9.1. В ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» действует трехступенчатая система контроля выполнения требований по защите сведений, составляющих персональные данные – текущий, периодический и внеплановый контроль.

9.2.Текущий контроль заключается:

- в самоконтроле самими сотрудниками ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», допущенными к обработке персональных данных, правил обработки персональных данных в процессе работы;
- в ежедневном наблюдении за выполнением сотрудниками требований по обработке персональных данных в процессе работы, осуществляемом начальниками структурных подразделений.

9.3.Периодический контроль выполнения требований по защите персональных данных осуществляется специальными комиссиями, создаваемыми приказом директора ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза». Периодический контроль осуществляется на основании годовых планов проведения проверочных мероприятий, разрабатываемых ответственным над обеспечением безопасности персональных данных.

9.4. Внеплановый контроль проводится в следующих случаях:

- нарушения конфиденциальности, целостности, доступности персональных данных;
- выявления фактов халатности и несоблюдения требований к обеспечению безопасности персональных данных;
- обнаружения факта утраты носителей персональных данных;
- на основании обращений субъектов персональных данных.

9.5. В рамках проведения контрольных мероприятий выполняются:

1) Проверка наличия и актуальности планов, регистрационных журналов, договоров, актов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных.

2) Проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных.

3) Проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию.

4) Проверка наличия и исправности технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации.

5) Проверка сохранности носителей персональных данных.

6) Проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем.

7) Проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональных данных действующим требованиям законодательства РФ.

9.6 Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

10. Обязанности сотрудников, допущенных к обработке персональных данных

10.1.В целях обеспечения конфиденциальности информации, относящейся к персональным данным, сотрудники ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» обязаны:

- не разглашать и не использовать с целью получения выгоды персональные данные, которые будут доверены или станут им известны при выполнении должностных обязанностей;
- не передавать третьим лицам и не раскрывать публично персональные данные без письменного согласия субъекта персональных данных;
- выполнять требования приказов, положений, инструкций по обеспечению сохранности персональных данных в ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза»;
- об утрате или недостаче носителей сведений, в которых фигурируют персональные данные, ключей от хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях

возможной утечки сведений немедленно сообщать руководителю или ответственному за обеспечение безопасности персональных данных;

- передать директору при прекращении или расторжении трудового договора, имеющиеся в пользовании материальные носители, содержащие персональные данные;

- информировать директора ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» о допущенных нарушениях установленного порядка обработки персональных данных, а также о фактах неправомерного использования таких сведений.

10.2.Выполнять требования Инструкции пользователя информационной системы персональных данных.

11. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

11.1. Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

11.2. Директор ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», разрешающий доступ работника к персональным данным, несет персональную ответственность за данное разрешение.

11.3. Директор ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза» за нарушение норм, регулирующих получение, обработку и защиту персональных данных несет административную ответственность согласно статьям 5.27, 5.39 и 13.11 Кодекса об административных правонарушениях Российской Федерации.

11.4. Работник ПОЧУ «Ижевский техникум экономики, управления и права Удмуртпотребсоюза», получающий для работы документ, содержащий персональные данные, несет ответственность за сохранность носителя и конфиденциальность информации.

11.5. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

11.6. Должностные лица, в обязанность которых входит обработка персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с его персональными данными и содержащими эти данные документами и материалами, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке

документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо представление неполной или заведомо ложной информации влечет привлечение должностных лиц к административной ответственности в порядке, определяемом Кодексом об административных правонарушениях.

11.7. В соответствии с Гражданским кодексом, лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

11.8. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения, наступает в порядке, установленном Уголовным кодексом.

Юрисконсульт **Т.Ю. Касаткина**

Администратор безопасности **Е.В. Вахрушева**

Ознакомлены: