Приложение№1 к приказу от « 01» сентября 2017 года № 144-а « О введении в действие Концепции информационной безопасности персональных данных КГБПОУ «Красноярский строительный техникум»

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ КГБПОУ «КРАСНОЯРСКИЙ СТРОИТЕЛЬНЫЙ ТЕХНИКУМ»

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИСПДн – информационная система персональных данных
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
УБПДн – угрозы безопасности персональных данных

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая Концепция информационной безопасности персональных данных (далее – Концепция) КГБПОУ «Красноярский строительный техникум» (далее - Техникум) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Политике информационной безопасности ИСПДн Техникума.

2.2. Концепция разработана в соответствии с требованиями ФЗ от 27.07.2006 №152-ФЗ «О персональных данных», а также других подзаконных актов, регулирующих сферу защиты информации.

2.3. В Концепции определены требования к ИСПДн, степень ответственности персонала, требования к системе защиты, статус и обязанности сотрудников Техникума по защите ПДн.

2.4. Концепция информационной безопасности ПДн определяет стратегию Техникума в области ИБ ПДн, а также те меры и средства, которые целесообразно применять для их защиты от несанкционированного доступа.

2.5. Целью настоящей Концепции является обеспечение безопасности ПДн, циркулирующих в информационных системах Техникума, от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз ПДн (УБПДн).

2.6. Настоящая Концепция направлена на:

- соблюдение интересов субъектов ПДн, Техникума и государства в информационной сфере;
- соответствие процессов сбора, накопления, обработки и предоставления ПДн нормам законодательства РФ;

- реализацию персональной ответственности за нарушения информационной безопасности;
- предотвращение и нейтрализацию угроз информационной безопасности Техникума;
- постоянный системный подход к контролю состояния информационной безопасности Техникума;

3. ОБЛАСТЬ ДЕЙСТВИЯ

3.1. Концепция информационной системы безопасности затрагивает все виды деятельности Техникума, касающиеся сбора, обработки, накопления, предоставления и распространения ПДн. Предметом настоящей Концепции ИСПДн Техникума являются:

- персональные данные, представленные в виде документированной информации на различных рода носителях, информационных массивах и базах данных, подлежащих защите в соответствии с законодательством РФ и внутренними организационно-распределительными документами Техникума.
- средства и системы информатизации, программные средства, автоматизированные системы управления, информационные и технологические процессы, используемые для обработки ПДн.

3.2. Выполнение положений Концепции информационной безопасности является обязательным для всех сотрудников Техникума. Взаимоотношения по использованию положений настоящего документа применительно к защите информации, находящейся в совместном ведении с другими организациями, регулируются на основании специальных соглашений.

4. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Система защиты персональных данных разрабатывается на основании:

- федеральных законов, Указов Президента, Постановлений Правительства РФ, приказов и положениях ФСТЭК России, ФСБ России, Минкомсвязи России и других нормативно-правовых актов, регулирующих область защиты информации.
- модели угроз безопасности Техникума.
- перечня персональных данных, подлежащих защите.
- классификации угроз информационной системы персональных данных.

4.2. Система защиты ПДн и организация основывается на:

- использовании ПДн только в соответствии с целями их обработки в Техникуме.
- регламентации порядка доступа к информационным ресурсам.
- определении прав доступа к информационным ресурсам их владельцами.
- применении антивирусных и иных средств защиты информации.

4.3. СЗПДн Техникума должна обеспечивать:

- защиту серверов за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, серверам регистрации и учета событий, связанных с осуществлением доступа к ресурсам серверов, механизмов мониторинга и аудита безопасности.

- комплексную антивирусную защиту систем, входящих в состав ИСПДн, за счет распределения антивирусных средств (антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по всем узлам системы.

4.4. Для обеспечения безопасности СЗПДн необходимо использовать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов.
- средства идентификации пользователей.
- средства физического разграничения доступа в защищаемые помещения.
- другие средства, направленные на обеспечение информационной безопасности.

5. МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Комплекс мер по защите в Техникуме включает в себя следующие мероприятия:

- назначение и распределение ответственности.
- разработка, реализация, внедрение и контроль исполнения планов мероприятий и других документов по обеспечению информационной безопасности.
- аудит информационной безопасности Техникума.

5.2. Концепция защиты ИСПДн Техникума реализуется путем сочетания организационных и технических мер, направленных на защиту ИСПДн. К организационным мерам защиты ИСПДн относятся:

- управление персоналом.
- физическая защита объекта.
- поддержание работоспособности.
- инвентаризация информационных ресурсов Техникума.
- реагирование на нарушение режима безопасности.
- планирование восстановительных работ.

5.3. Реагирование на нарушение режима безопасности должно предусматривать набор оперативных мероприятий, положений, должностных инструкций, направленных на обнаружение и нейтрализацию угрозы. Общее руководство информационной безопасностью в Техникуме осуществляет исполнительный директор.

5.4. Работы по обеспечению информационной безопасности осуществляет ответственный за обработку персональных данных.

6. ОБЯЗАННОСТИ СОТРУДНИКОВ ТЕХНИКУМА ПО ЗАЩИТЕ ПДн:

Описание обязанностей всех сотрудников Техникума по обработке и защите ПДн закреплены в Инструкции по работе в информационной системе, содержащей ПДн.

6.1. Сотрудники Техникума обязаны в незамедлительном порядке информировать о ставших им известными фактах нарушений положений настоящей Концепции и инцидентах информационной безопасности своего непосредственного руководителя, ответственного за организацию работ по защите информации или руководство Техникума.

6.2. Ответственный за обработку персональных данных обязан инициировать и проводить служебные расследования по факту нарушений и инцидентов информационной безопасности в соответствии с установленной в Техникуме процедурой и докладывать о результатах расследований руководству Техникума.

7. ОТВЕТСТВЕННОСТЬ

7.1. В соответствии с ФЗ от 27.07.2006 г. №152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного ФЗ, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

7.2. 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 (статьи 272, 273 и 274 УК РФ), несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.