П-129/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____ А.Н. Сакеев
«29» октября 2019г.

Приказ № 522 о/д от 29.10.2019

Положение об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Настоящее положение определяет порядок организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ГБПОУ «ТК им. Н.Д. Кузнецова» (далее - Учреждение).

1.2. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»,
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»,
- Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных",
- Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- Приказом ФАПСИ от 13.06.2001 № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну";
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.3. Для целей настоящего Положения применяются следующие термины и определения:

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

Оператор Персональных данных - Учреждение — 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.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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, 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.

Пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа к информационным системам персональных данных - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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.

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.

Конфиденциальность персональных данных - Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного

государства, иностранному физическому лицу или иностранному юридическому лицу.

Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Защита информации - комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

- разграничение полномочий доступа к данным;
- авторизация, контроль и учет действий с данными (регистрация событий);
- контроль копирования, печати, обмена данными по каналам связи;
- межсетевое экранирование и защита от вирусов;
- учет внешних носителей данных;
- резервное копирование / восстановление данных;
- раздельное хранение носителей данных с резервными копиями;
- контроль доступа в помещения и к компьютерам;
- применение устройств идентификации пользователей для доступа.

1.4. Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных - ИСПДн) достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

1.5. Мероприятия по обеспечению безопасности ПДн формулируются на основании анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

1.6. Обеспечение безопасности ПДн осуществляется путем выполнения Требований по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения (Приложение № 1).

1.7. Структура, состав и основные функции СЗПДн определяются исходя из анализа типа актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

1.8. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн; на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

1.9. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн,

предусмотренных для соответствующего уровня защищенности информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с ПДн в информационной системе;

з) контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

1.10. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.11. Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

1.12. По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автоматизированного рабочего места;
- угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем;
- угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования.

1.13. Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

- обследование и оформление документа о типе актуальных угроз и уровней защищенности персональных данных, обрабатываемых в ИСПДн, определение способов и состава средств защиты информации (СЗИ), разработка технического задания (ТЗ) на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование;
- ввод в эксплуатацию - закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентов обработки конфиденциальной информации

2. Цели обеспечения информационной безопасности.

2.1. Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

- целостности информации;
- доступности обрабатываемой информации для зарегистрированных пользователей;
- конфиденциальности информации

3. Объект защиты.

3.1. Объектом защиты является информационная система персональных данных работников, обучающихся и их родителей (законных представителей) Учреждения:

а) Информационные ресурсы:

- персональные данные работников, обучающихся и их родителей (законных представителей) (исходная информация, информационные базы данных);
- инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;

б) технические информационные системы и средства Учреждения, в которых обрабатывается, хранится и передается информация ПДн;

в) помещения объектов Учреждения, в которых размещаются информационные ресурсы, и обрабатывается конфиденциальная информация;

г) технические системы жизнеобеспечения, электропитания, проводного вещания, охранной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн.

3.2. Критичными свойствами объекта защиты являются:

а) возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;

б) возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;

в) несанкционированная доступность информации, выражающаяся в возможности:

- непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на носитель или транспортную среду с целью перлюстрации, отчуждения, копирования, изменения, подмены и уничтожения информации;
- прямого или косвенного доступа к оборудованию ИСПДн и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ);
- перехвата речевой информации по акустическим и другим каналам утечки (подслушивание).

4. Субъекты информационных отношений

4.1. Субъектами информационных отношений являются:

- Работники (субъекты) - физические лица, состоящие в трудовых и иных гражданско-правовых отношениях с Учреждением-оператором;
- Обучающиеся (субъекты персональных данных) - физические лица, которые состоят в договорных и иных гражданско-правовых отношениях с Учреждением-оператором по вопросам оказания услуг в сфере образования, предусмотренных Уставом.

4.2. Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности (сохранения в тайне) информации в соответствии с требованиями российского законодательства;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);

- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты информации от незаконного ее тиражирования (защиты персональных

доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты.

Меры безопасности ПДн должны гарантировать:

- конфиденциальность;
- целостность;
- доступность информации.

Мероприятия по обеспечению безопасности предусматривают:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия;
- анализ защищенности.

Подсистемы управления доступом и регистрации и учета должны реализовываться на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы программные и программно-аппаратные средства защиты самих операционных систем, электронных баз данных и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных действий пользователя или нарушителя.

Средства диагностики должны осуществлять тестирование файловой системы и баз данных, постоянный сбор информации о функционировании элементов подсистемы обеспечения безопасности информации.

Средства уничтожения предназначены для уничтожения остаточных данных и должны предусматривать аварийное уничтожение данных в случае угрозы несанкционированного доступа (НСД), которая не может быть блокирована системой.

Средства сигнализации предназначены для предупреждения операторов (пользователей) при их обращении к защищаемым данным и для предупреждения администратора при обнаружении факта НСД, искажении программных средств защиты, выходе или выводе из строя аппаратных средств защиты и о других фактах нарушения штатного режима функционирования.

Подсистема обеспечения целостности должна быть реализована операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

Подсистема контроля отсутствия недекларированных возможностей должна

безопасности информации.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных в информационных системах персональных данных.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, должны допускаться к соответствующим персональным данным на основании утвержденных Перечней должностных лиц, допущенных к работе с персональными данными.

Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в утвержденных Перечнях должностных лиц, а также факты предоставления персональных данных по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) Учреждения или уполномоченными лицами.

При обнаружении нарушений порядка предоставления персональных данных Учреждения уполномоченные лица должны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

При хранении материальных носителей информации с персональными данными (или другой конфиденциальной информацией) должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются отдельно.

Приложение 2
к Положению об организации работ по
обеспечению безопасности персональных данных
при их обработке в информационных системах
персональных данных

РЕКОМЕНДАЦИИ
по использованию программных и аппаратных средств защиты информации и обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Мероприятия по защите ПДн при их обработке в ИСПДн от несанкционированного доступа и неправомерных действий включают в себя:

- управление доступом;
- регистрацию и учет;
- обеспечение целостности;
- контроль отсутствия недекларированных возможностей;
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия ИСПДн;
- анализ защищенности;
- обнаружение вторжений.

Для выполнения вышеназванных требований, необходимо наличие следующих средств защиты:

- средство защиты от несанкционированного доступа;
- межсетевой экран;
- антивирус.

При выборе того или иного средства защиты основными критериями отбора являются:

- наличие сертификатов ФСТЭК, ФСБ;
- обеспечение необходимого уровня защиты;
- производительность;
- совместимость;
- простота настройки и эксплуатации;
- техническая поддержка;
- цена.