

Муниципальное бюджетное учреждение
дополнительного образования
Спортивная школа Жердевского муниципального округа

Принято на заседании
педагогического совета
от «05» февраля 2024г.
протокол № 1

УТВЕРЖДЕНО
Приказом МБУ ДО
Спортивная школа Жердевского
муниципального округа
от «05» февраля 2024г. приказ № 6

ПОЛИТИКА
МБУ ДО Спортивная школа Жердевского муниципального округа в
отношении обработки персональных данных

1.Содержание

Обозначения и сокращения:

ИСПД – информационная система персональных данных.

НСД - несанкционированный доступ.

ПД – персональные данные.

Политика – политика образовательных учреждений в отношении обработки персональных данных.

СЗПД – система защиты персональных данных.

ТЗКИ – техническая защита конфиденциальной информации.

ТС – техническое средство.

Термины и определения:

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

Безопасность информации – состояние защищенности информации, характеризуемое способностью технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного доступа, распространения и самовоспроизведения.

Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Накопитель информации – устройство, предназначенное для записи и (или) чтения информации на носитель информации. Накопитель информации конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначен для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт).

Встроенные накопители подразделяются на съемные и несъемные.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке (в том числе техническими средствами) в информационных системах персональных данных. Несанкционированный доступ (несанкционированные действия) – 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 функциональному назначению и техническим характеристикам.

Носитель информации – физический объект, предназначенный для хранения 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. 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.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

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

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

Система защиты персональных данных – комплекс организационных мер и программно - технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПД.

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.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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.

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.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

1. Основные положения

1.1. Настоящая Политика устанавливает порядок организации и проведения работ по защите информации в ИСПД, создаваемых и эксплуатируемых в образовательном учреждении.

1.2. Требования настоящей Политики распространяются на защиту информации с ограниченным доступом, отнесенной к информации, составляющей ПД.

1.3. Политика является дополнением к действующим в РФ нормативным документам по вопросам обеспечения информационной безопасности ПД, и не исключает обязательного выполнения их требований.

1.4. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПД образовательных учреждений, а также нормативных и методических документов, обеспечивающих ее реализацию.

1.5. Политика определяет следующие основные вопросы защиты информации:

- основные принципы и требования по защите информации, составляющей ПД;
- порядок организации и проведения работ по защите информации;
- порядок обеспечения защиты информации при эксплуатации ИСПД;
- порядок организации делопроизводства, хранения и обращения накопителей и носителей информации.

2. Принципы обеспечения защиты информации, составляющей персональные данные

2.1. Законность — предполагает обеспечение защиты ПД в соответствии с действующим в РФ законодательством и нормативными актами в области защиты ПД.

Пользователи и обслуживающий персонал ИСПД должны быть осведомлены о правилах и порядке работы с защищаемой информацией и об ответственности за их нарушение.

2.2. Системность — предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПД ИСПД.

2.3. Комплексность — предполагает согласованное применение разнородных средств и систем при построении комплексной системы защиты информации, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

2.4. Непрерывность — предполагает функционирование СЗПД в виде непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла ИСПД. ИСПД должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры не допускающие переход ИСПД в незащищенное состояние.

2.5. Своевременность — предполагает упреждающий характер мер обеспечения безопасности ПД, то есть постановку задач по комплексной защите ИСПД и реализацию мер обеспечения безопасности ПД на ранних стадиях разработки ИСПД в целом и ее системы защиты информации, в частности.

2.6. Совершенствование — предполагает постоянное совершенствование мер и средств защиты информации на основе комплексного применения организационных и технических решений, квалификации персонала, анализа функционирования ИСПД и ее системы защиты с учетом изменений условий функционирования ИСПД, появления новых методов и средств перехвата информации, изменений требований нормативных документов по защите ПД.

2.7. Персональная ответственность — предполагает возложение ответственности за обеспечение безопасности ПД и ИСПД на каждого исполнителя в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей исполнителей строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

2.8. Минимальная достаточность — предполагает предоставление исполнителям минимально необходимых прав доступа к ресурсам ИСПД в соответствии с производственной необходимостью, на основе принципа «запрещено все, что не разрешено явным образом».

2.9. Гибкость системы защиты — предполагает наличие возможности варьирования уровнем защищенности при изменении условий функционирования ИСПД.

2.10. Обязательность контроля — предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПД на основе используемых систем и средств защиты информации.

Контроль за деятельностью каждого пользователя, каждого средства защиты и в отношении каждого объекта защиты должен осуществляться на основе применения средств контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

3. Основные требования по защите информации составляющей персональные данные

3.1. Защита информации в ИСПД является неотъемлемой составной частью управленческой и научной деятельности образовательного учреждения и должна осуществляться во взаимосвязи с другими мерами по защите информации, составляющей ПД.

3.2. Защита информации является составной частью работ по созданию и эксплуатации ИСПД и должна осуществляться в установленном настоящей Политикой порядке и реализовываться в виде системы (подсистемы) защиты ПД.

3.3. Защита информации должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счет НДС к ней, по предупреждению преднамеренных программно - технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее санкционированной доступности и работоспособности ТС.

3.4. В ИСПД должны использоваться сертифицированные по требованиям безопасности информации средства защиты информации и (или) технические и организационные решения, исключающие утечку информации по техническим каналам, за счет НСД, предупреждающие нарушение целостности информации и ее санкционированной доступности.

3.5. Защита информации должна быть дифференцированной в зависимости от применяемых технических средств, обрабатывающих информацию, составляющую ПД, установленного класса ИСПД и утвержденной для ИСПД модели угроз.

3.6. Все используемые в ИСПД средства защиты информации должны быть проверены на соответствие ограничениям и условиям эксплуатации, изложенным в сертификате соответствия, эксплуатационной документации или формуляре (для технических и программных средств защиты информации соответственно).

3.7. Обработка информации составляющей ПД осуществляется на основании письменного разрешения (приказа) руководителя образовательного учреждения, в котором эксплуатируется ИСПД.

3.8. Ответственность за обеспечение выполнения установленных требований по защите информации возлагается на руководителя образовательного учреждения, в котором создается (совершенствуется) и эксплуатируется ИСПД.

3.9. Все ИСПД должны пройти оценку эффективности принимаемых мер по обеспечению безопасности ПД до начала обработки информации составляющей ПД.

4. Порядок организации и проведения работ по защите информации.

4.1. Организация работ по защите информации возлагается на руководителя образовательного учреждения, осуществляющего разработку (модернизацию) и эксплуатацию ИСПД.

4.2. Организация и проведение работ по защите информации, составляющей ПД на различных стадиях разработки, внедрения и эксплуатации ИСПД определяется действующими в РФ нормативными документами и настоящим документом.

4.3. Проведение работ по защите информации, составляющей ПД, осуществляется силами образовательного учреждения, в котором создается (совершенствуется) ИСПД. В случае невозможности или нецелесообразности выполнения работ по защите информации силами образовательного учреждения к этим работам должна привлекаться специализированная организация, имеющая соответствующие лицензии на право выполнения работ и оказания услуг по ТЗКИ.

4.4. Стадии создания системы защиты информации:

- предпроектная стадия — включает предпроектное обследование создаваемой ИСПД;
- разработку аналитического обоснования необходимости создания системы защиты информации и технического задания на ее создание.
- стадия проектирования (разработки проектов) и реализации ИСПД — включает разработку СЗПД в составе ИСПД.

- Стадия ввода в действие системы СЗПД — включает опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку эффективности принимаемых мер по обеспечению безопасности ПД.

5. Порядок обеспечения защиты информации при эксплуатации ИСПД.

5.1. Эксплуатация ИСПД должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией ИСПД.

5.2. Ответственность за обеспечение защиты информации в процессе эксплуатации ИСПД возлагается на руководителя образовательного учреждения, в ведении которого находится эта ИСПД.

5.3. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИСПД возлагается на непосредственных исполнителей ИСПД (пользователей, администраторов, обслуживающий персонал).

5.4. За нарушение установленных требований по защите информации руководитель образовательного учреждения, в ведении которого находится ИСПД и (или) непосредственный исполнитель привлекаются к ответственности в соответствии с действующим в РФ законодательством.

6. Порядок организации делопроизводства, хранения и обращения накопителей и носителей информации

6.1. Все накопители и носители информации содержащие ПД на бумажной, магнитной, магнито - оптической и иной основе, используемые в технологическом процессе обработки информации в ИСПД, подлежат учету, хранению и обращению в соответствии с требованиями конфиденциального делопроизводства.

6.2. Организация и ведение учета накопителей и носителей ПД, организация их хранения, обращения и уничтожения осуществляются ответственными делопроизводителями конфиденциального делопроизводства.

6.3. ПД, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПД, в специальных разделах или на полях форм (бланков).

6.4. При фиксации ПД на материальных носителях не допускается фиксация на одном материальном носителе ПД, цели обработки которых заведомо не совместимы.

6.5. Для обработки различных категорий ПД, осуществляемой без использования средств автоматизации, для каждой категории ПД должен использоваться отдельный материальный носитель.

6.6. Обработка ПД без использования средств автоматизации должна осуществляться таким образом, чтобы в отношении каждой категории ПД можно было определить места хранения ПД (материальных носителей) и установить перечень лиц, осуществляющих обработку ПД либо имеющих к ним доступ.

6.7. Должно обеспечиваться раздельное хранение ПД (материальных носителей), обработка которых осуществляется в различных целях.

6.8. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПД и исключающие несанкционированный к ним доступ.

7. Контроль состояния и эффективности защиты ИСПД.

7.1. В ИСПД должен осуществляться контроль и (или) аудит соответствия обработки ПД действующим в РФ законодательству и требованиям к защите ПД, а так же настоящей Политике и локальным актам образовательного учреждения.

7.2. Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению ПД.

7.3. Контроль подразделяется на оперативный и плановый (периодический).

7.4. В процессе эксплуатации ИСПД в целях защиты информации от НСД осуществляются оперативный контроль и периодический контроль за выполнением исполнителями требований действующих нормативных документов по вопросам обеспечения безопасности и защиты ПД.

7.5. С целью своевременного выявления и предотвращения утечки информации, исключения или существенного затруднения НСД и предотвращения специальных воздействий (программно-технических и др.), вызывающих нарушение целостности информации или работоспособность технических средств, в ИСПД образовательных учреждений проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

7.6. При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности ИСПД от утечки ПД по техническим каналам, выборочный контроль содержимого накопителей и носителей информации, и т.п.

7.7. Результаты контроля оформляются актами, заключениями и записями в эксплуатационной документации.