Государственное автономное образовательное учреждение
профессионального образования
«Училище олимпийского резерва Пензенской области»

УТВЕРЖДАЮ

Директор ГАОУ ПО

«Училище олимпийского резерва Пензенской области»

_____ Андреев В.М.

«__» _____ 2016 г.

ПОЛИТИКА

ГАОУ ПО «Училище олимпийского резерва Пензенской области»

в отношении обработки персональных данных

2016 г.

Содержание

Обозначения и сокращения

ИСПДн – информационная система персональных данных.

НСД - несанкционированный доступ.

ПДн – персональные данные.

Политика – политика ГАОУ СПО «Училище олимпийского резерва Пензенской области» в отношении обработки персональных данных.

СЗПДн – 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 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.

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.

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).

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

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных 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, использующей персональные данные в ГАОУ ПО «Училище олимпийского резерва Пензенской области» (далее — образовательное учреждение).

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

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

1.4. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПДн образовательного учреждения, 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 ПДн,
- порядок организации и проведения работ по защите информации,
- порядок организации делопроизводства, хранения и обращения носителей информации.

2. Принципы обеспечения защиты информации, составляющей персональные данные

Защита информации, составляющей ПДн должна осуществляться в соответствии со следующими основными принципами:

2.1. Законность — предполагает обеспечение защиты ПДн в соответствии с действующим в РФ законодательством и нормативными актами в области защиты ПДн. Пользователи и обслуживающий персонал 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 ПДн.

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 СЗПДн в виде непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла ПДн. ПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом

должны приниматься меры не допускающие переход ПДн в незащищенное состояние.

2.5. Своевременность — предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ПДн и реализацию мер обеспечения безопасности ПДн 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 ПДн и ее системы защиты с учетом изменений условий функционирования ПДн, появления новых методов и средств перехвата информации, изменений требований нормативных документов по защите ПДн.

2.7. Персональная ответственность — предполагает возложение ответственности за обеспечение безопасности ПДн 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 ПДн 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 использования ПДн.

2.10. Обязательность контроля — предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе

используемых систем и средств защиты информации. Контроль за деятельностью каждого работника, 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 работников.

3. Основные требования по защите информации составляющей персональные данные

3.1. Защита информации персональных данных является неотъемлемой составной частью управленческой и научной деятельности образовательного учреждения и должна осуществляться в комплексе с другими мерами по защите информации, составляющей ПДн.

3.2. Защита информации является составной частью работ по использованию и обработке ПДн и должна осуществляться в установленном настоящей Политикой порядке и реализовываться в виде системы (подсистемы) защиты ПДн.

3.3. Защита информации должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации, за счет НСД к ней, по предупреждению преднамеренных действий третьих лиц с целью неправомерного завладения ею.

3.4. Защита информации должна быть дифференцированной в зависимости от применяемых способов обработки ПДн.

3.5. Обработка информации составляющей ПДн осуществляется на основании письменного разрешения (приказа) руководителя образовательного учреждения.

3.6. Ответственность за обеспечение выполнения установленных требований по защите информации ПДн, возлагается на руководителя образовательного учреждения.

3.7. Все средства и способы защиты ПДн должны пройти оценку эффективности принимаемых мер по обеспечению безопасности ПДн до начала обработки информации составляющей ПДн.

4. Порядок организации и проведения работ по защите информации

4.1. Организация работ по защите информации, содержащей ПДн, собираемой и обрабатываемой в организации, возлагается на руководителя образовательного учреждения.

4.2. Организация и проведение работ по защите информации, составляющей ПДн определяется действующими в РФ нормативными документами и настоящим документом.

4.3. Проведение работ по защите информации, составляющей ПДн, осуществляется силами образовательного учреждения. 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.

5. Порядок организации делопроизводства, хранения и обращения носителей информации

5.1. Все носители информации, содержащие ПДн на бумажной или иной основе, используемые в процессе обработки информации, подлежат учету, хранению и обращению в соответствии с требованиями конфиденциального делопроизводства.

5.2. Организация и ведение учета носителей ПДн, организация их хранения, обращения и уничтожения осуществляются ответственными делопроизводителями конфиденциального делопроизводства.

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

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

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

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

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

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

6. Контроль состояния и эффективности защиты ПДн

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

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

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

6.4. В процессе эксплуатации ПДн 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 ПДн.

6.5. С целью своевременного выявления и предотвращения утечки информации, исключения или существенного затруднения НСД и предотвращения специальных воздействий, вызывающих нарушение целостности информации, в отделах, обрабатывающих ПДн, образовательного учреждения проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

6.6. При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности ПДн от утечки, выборочный контроль содержимого носителей информации, и т.п.

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