Приложение 1
к приказу Генерального директора
АНО ДПО «ИСЗ» № 2 от «10» августа 2024 г.

ПОЛИТИКА

образовательного учреждения

в отношении обработки персональных данных

Обозначения и сокращения

ИСПДн – информационная система персональных данных.

НСД - несанкционированный доступ.

ПДн – персональные данные.

Политика – политика образовательных учреждений 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.

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 предназначению 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 ИСПДн.

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.

ОСНОВНЫЕ ПОЛОЖЕНИЯ

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

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

1.3. Политика является дополнением к действующим 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 обеспечения защиты информации при эксплуатации ИСПДн,

- порядок организации делопроизводства, хранения и обращения накопителей и носителей информации.

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

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

1.6. Законность — предполагает обеспечение защиты ПДн в соответствии с действующим в РФ законодательством и нормативными актами в области защиты ПДн. Пользователи и обслуживающий персонал ИСПДн должны быть осведомлены о правилах и порядке работы с защищаемой информацией и об ответственности за их нарушение.

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

1.8. 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.

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

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

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

1.12. Персональная ответственность — предполагает возложение ответственности за обеспечение безопасности ПДн и ИСПДн 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.

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

1.14. Гибкость системы защиты — предполагает наличие возможности варьирования уровнем защищенности при изменении условий функционирования ИСПДн.

1.15. 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 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.

ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

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

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

1.18. Защита информации должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счет НСД 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.

1.19. В ИСПДн 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.

1.20. Защита информации должна быть дифференцированной в зависимости от применяемых технических средств, обрабатывающих информацию, составляющую ПДн, установленного класса ИСПДн и утвержденной для ИСПДн модели угроз.

1.21. Все используемые в ИСПДн 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).

1.22. Обработка информации, составляющей ПДн осуществляется на основании письменного разрешения (приказа) руководителя образовательного учреждения, в котором эксплуатируется ИСПДн. Ответственность за обеспечение выполнения установленных требований по защите информации возлагается на руководителя образовательного учреждения, в котором создается (совершенствуется) и эксплуатируется ИСПДн. Все ИСПДн должны пройти оценку эффективности принимаемых мер по обеспечению безопасности ПДн до начала обработки информации, составляющей ПДн.

ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

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

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

1.25. Проведение работ по защите информации, составляющей ПДн, осуществляется силами образовательного учреждения, в котором создается (совершенствуется) ИСПДн. 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.

1.26. Стадии создания системы защиты информации:

1.27. Предпроектная стадия — включает предпроектное обследование создаваемой ИСПДн, разработку аналитического обоснования необходимости создания системы защиты информации и технического задания на ее создание.

1.28. Стадия проектирования (разработки проектов) и реализации ИСПДн — включает разработку СЗПДн в составе ИСПДн.

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

ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ИСПДН

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

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

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

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

ПОРЯДОК ОРГАНИЗАЦИИ ДЕЛОПРОИЗВОДСТВА, ХРАНЕНИЯ И ОБРАЩЕНИЯ НАКОПИТЕЛЕЙ И НОСИТЕЛЕЙ ИНФОРМАЦИИ

Все накопители и носители информации, содержащие ПДн на бумажной, магнитной, магнитооптической и иной основе, используемые в технологическом процессе обработки

информации в ИСПДн, подлежат учету, хранению и обращению в соответствии с требованиями конфиденциального делопроизводства.

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

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

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

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

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.

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

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

КОНТРОЛЬ СОСТОЯНИЯ И ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИСПДН

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

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

Контроль подразделяется на оперативный и плановый (периодический).

В процессе эксплуатации ИСПДн 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.

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 ИСПДн образовательных учреждений проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

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

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

Приложение 2
к приказу Генерального директора
АНО ДПО «ИСЗ» № 2 от «10» августа 2024 г.

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ ОТНОШЕНИИ ПОЛЬЗОВАТЕЛЕЙ САЙТА HTTPS://ANOISZ.RU

1.1. Настоящая политика конфиденциальности действует в отношении персональных данных, которые АНО ДПО «ИСЗ» может получить о пользователях его официального сайта https://anoisz.ru (далее – Сайт), во время посещения ими страниц и разделов Сайта, а также при использовании ими форм ввода данных, расположенных на Сайте.

1.2. В настоящей Политике конфиденциальности используются следующие

1 2.1. Пользователи Сайта (далее – Пользователи) – лица, имеющие доступ к Сайту, посредством сети Интернет, посещающие его страницы и разделы и (или) пользующиеся формами ввода данных, расположенными на Сайте;

1.2.2. Персональные данные – любая информация, относящаяся прямо или косвенно к пользователям Сайта;

1 2.3. АНО ДПО «ИСЗ» (далее – Оператор) – владелец доменного имени https://anoisz.ru, оператор обработки персональных данных пользователей Сайта, самостоятельно поддерживает функционирование Сайта, непосредственно организует и (или) осуществляет обработку персональных данных пользователей Сайта, а также определяет цели обработки их персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

1.2.5. 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;

1.2.6. Конфиденциальность персональных данных – обязательное для соблюдения Оператором требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

1.2.7. Cookies — фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя, который веб-клиент или веб-браузер каждый раз пересылает веб-серверу в HTTP-запросе при попытке открыть страницу соответствующего сайта;

1.2.8. IP-адрес — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

1.3. Политика разработана в соответствии с Федеральным Законом от 27.07.2006 №152-ФЗ «О персональных данных», Уставом АНО ДПО «ИСЗ».

1.4. Обработка персональных данных пользователей осуществляется Оператором исключительно в следующих целях:

1.4.1 Повышение качества функционирования Сайта, совершенствования его структуры;

1.4.2. Идентификация пользователей, использующих формы ввода данных, для связи с ними со стороны Оператора;

1.4.3. Направление уведомлений, запросов и информации, а также обработки запросов и заявок от пользователей, использующих формы ввода данных;

1.4.4. Формирования статистической отчетности и проведения иных исследований, на основе обезличенных данных.

1.5. Настоящая Политика утверждается приказом Генерального директора АНО ДПО «ИСЗ» и действует до его отмены или принятия новой Политики. Оператор вправе вносить изменения в настоящую Политику конфиденциальности без согласия Пользователей.

2. РАБОТА С ПЕРСОНАЛЬНЫМИ ДАННЫМИ ПОЛЬЗОВАТЕЛЕЙ

2.1. При просмотре Сайта, чтении страниц Сайта или при загрузке информации с Сайта Оператор автоматически собирает и сохраняет анонимную информацию о посещении (посещениях) пользователями Сайта. Собираемая информация не содержит данных, которые могут позволить идентифицировать личность пользователя Сайта.

2.1.1. При посещении Сайта Оператор с помощью сервиса «Яндекс Метрика» собирает и сохраняет следующую обобщенную информацию:

• Интернет-домен или IP адрес, с которого пользователь осуществил доступ к Сайту;

• Информация из cookies;

• Тип интернет-браузера и операционной системы, которые пользователь использует для доступа к Сайту;

• Дата и время посещения (посещений), длительность посещения (посещений).

2.2. Оператор хранит обезличенные персональные данные пользователей на сервисе «Яндекс Метрика». Доступ к персональному компьютеру, с помощью которого осуществляется доступ к сервису, ограничен паролем, известным ответственным по работе с персональными данными сотрудникам Оператора. Срок хранения данных составляет 3 года.

2.3. При использовании форм ввода данных автоматически фиксируется IP-адрес пользователя, прочие персональные данные фиксируются в объёме, предусмотренном конкретной формой.

2.4. Сбор и хранение персональных данных пользователей, воспользовавшихся формами ввода данных, осуществляется в автоматическом режиме на сервере. Срок хранения данных составляет 5 лет.

3. СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Посещая страницы и разделы Сайта, а также заполняя формы ввода данных, пользователь выражает своё согласие с настоящей Политикой и указанными в ней условиями, целями обработки его персональных данных. В случае несогласия с этими условиями и целями обработки персональных данных, пользователь должен воздержаться от использования Сайта.

3.2. Пользователь гарантирует, что предоставленная с помощью форм ввода данных информация является полной, точной и достоверной, она не нарушает действующее законодательство РФ, законные права и интересы третьих лиц и заполнена в отношении себя лично. Оператор не проверяет достоверность персональных данных, предоставляемых пользователями Сайта.

4 Дополнительные условия

4.1. Все предложения или вопросы по настоящей Политике конфиденциальности следует сообщать на адрес operator@anoisz.ru

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 02D2367300C7B17DA449D00A0064A428D6
Владелец: КЕЛАРЕВ АРКАДИЙ ВЯЧЕСЛАВОВИЧ
Действителен: с 09.08.2024 до 09.11.2025