

ПРИНЯТО

На Педагогическом совете

протокол № 1 от 28.08.2021г.

УТВЕРЖДЕНО

приказом директора

от 31.08.2021 г. №135-од

Положение

о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах.

1. Термины, определения и сокращения

- 1.1. Автоматизированная информационная система (АС) - система, состоящая из работников и комплекса средств автоматизации их деятельности, реализующая информационную технологию выполнения установленных функций.
- 1.2. Администратор информационной системы персональных данных (администратор безопасности ИСПДн) - лицо, ответственное за сопровождение программного обеспечения информационной системы персональных данных.
- 1.3. Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.
- 1.4. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- 1.5. Вредоносная программа (ВП) - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.
- 1.6. Доступ к персональным данным - возможность получения персональных данных и их использования.
- 1.7. Защита от несанкционированного доступа - предотвращение или существенное затруднение несанкционированного доступа.
- 1.8. Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
- 1.9. Информация - сведения (сообщения, данные) независимо от формы их представления.
- 1.10. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.11. Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов.

1.12. Конфиденциальность персональных данных - обязательное для выполнения оператором и иным лицом, получившим доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.13. Несанкционированный доступ к персональным данным (несанкционированные действия), (НСД) - доступ к персональным данным или действия с персональными данными, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

1.14. 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.

1.15. Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

1.16. Оператор - муниципальный орган, самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

1.19. Пользователь ИСПДн - лицо, участвующее в функционировании ИСПДн или использующее результаты ее функционирования.

1.20. Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

1.21. Ресурс информационной системы персональных данных - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы персональных данных.

1.22. Средства вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки персональных данных, способных функционировать самостоятельно или в составе других систем.

1.23. Санкционированный доступ к персональным данным - доступ к персональным данным, не нарушающий правила разграничения доступа.

1.24. Система защиты персональных данных (СЗПДн) - комплекс организационных мер и программно-технических средств обеспечения безопасности ПДн в ИСПДн.

1.25. Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1.26. Технический канал утечки информации - совокупность носителя персональных данных (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается информация, содержащая персональные данные.

1.27. Технические средства информационной системы персональных данных (ТС) - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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).

1.28. 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.

1.29. 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.

1.30. Утечка (защищаемой) информации, содержащей персональные данные, по техническим каналам - неконтролируемое распространение персональных данных от носителя персональных данных через физическую среду до ТС, осуществляющего перехват информации, содержащей персональные данные.

1.31. Целостность информации, содержащей персональные данные, - способность средства вычислительной техники или информационной системы персональных данных обеспечивать неизменность информации, содержащей персональные данные, в условиях случайного и/или преднамеренного искажения (разрушения).

2. Общие положения.

2.1. Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Положение) разработано в соответствии с Конституцией Российской

Федерации, Федеральным законом "Об информации, информационных технологиях и защите информации", Федеральным законом "О персональных данных", постановлением Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", и определяет содержание и порядок осуществления мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн.

2.2. Настоящее Положение не регулирует вопросы обеспечения безопасности ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы обеспечения безопасности информации с ограниченным доступом (конфиденциальной), не содержащей ПДн.

2.3. Организация обеспечения безопасности ПДн при их обработке, осуществляющейся без использования средств автоматизации, возлагается на должностных лиц школы, утвержденных приказом директора.

2.4. Безопасность ПДн при их обработке в ИСПДн достигается путем исключения НСД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

2.5. Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью СЗПДн, включающей организационные меры и средства защиты информации (в том числе средства предотвращения НСД, утечки информации, содержащей ПДн, по техническим каналам, программно-технических воздействий на ТС обработки ПДн), а также используемые в ИСПДн школы информационные технологии.

2.6. Для обеспечения безопасности ПДн при их обработке в ИСПДн школы осуществляется защита речевой информации и информации, обрабатываемой ТС, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

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

2.8. Методы и способы защиты ПДн в ИСПДн школы устанавливаются Федеральной службой по техническому и экспортному контролю России и Федеральной службой безопасности России в пределах их полномочий.

2.9. Выбор методов, способов и средств защиты информации осуществляется в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю Российской Федерации.

2.11. Выбранные и реализованные в соответствии с п. 2.9 настоящего Положения методы и способы защиты информации в ИСПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПДн при их обработке в ИСПДн.

2.12. Достаточность принятых мер по обеспечению безопасности ПДн при их обработке в ИСПДн оценивается при проведении государственного контроля и надзора.

2.13. Мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн, включают в себя:

- определение требуемого уровня защищенности в соответствии с разделом 3 настоящего Положения;
- определение угроз безопасности ПДн при их обработке в ИСПДн ;
- разработку на основе определенных угроз безопасности ПДн частной модели угроз применительно к конкретной ИСПДн;
- разработку СЗПДн на основе частной модели угроз (СЗПДн обеспечивает нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищенности ИСПДн;
- проверку готовности средств защиты ПДн к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты ПДн в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты ПДн, применяемые в ИСПДн, правилам работы с ними;
- учет применяемых средств защиты ПДн, эксплуатационной и технической документации к ним, носителей ПДн;
- учет лиц, допущенных к работе с ПДн в ИСПДн;
- контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты ПДн, 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;
- описание СЗПДн.

2.14. В школе должен быть организован учет всех защищаемых носителей информации (как отчуждаемых (дискеты, диски и т.п.), так и неотчуждаемых (жесткие магнитные диски в составе системных блоков и т.п.)), на которых хранятся ПДн. Каждому защищаемому носителю информации присваивается свой учетный номер по Журналу учета и списания машинных носителей персональных данных.

Присвоенный защищаемому носителю информации номер проставляется также и на самом носителе.

2.15. Уничтожение ПДн осуществляется в следующих случаях:

- при выявлении неправомерных действий с ПДн и в случае невозможности устранения допущенных нарушений соответствующие ПДн уничтожаются в срок, не превышающий трех рабочих дней с даты такого выявления. Об устраниении допущенных нарушений или об уничтожении ПДн сотрудник, имеющий допуск, обязан в срок, не превышающий пяти рабочих дней с даты устраниния допущенных нарушений или уничтожения ПДн, уведомить ответственного за защиту информации или администратора безопасности;
- в случае достижения цели обработки ПДн либо утраты необходимости в такой цели соответствующие ПДн уничтожаются в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральными законами.
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн, соответствующие ПДн уничтожаются в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено действующим законодательством.

2.16. Размещение ИСПДн, специальное оборудование и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2.17. Лица, доступ которым к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (должностных) обязанностей, допускаются к соответствующим ПДн в порядке, установленном Регламентом.

2.18. Запросы пользователей ИСПДн на получение ПДн, включая лиц, указанных в п. 2.17 настоящего Положения, а также факты представления ПДн по этим запросам должны регистрироваться в журнале обращений. Содержание журнала обращений проверяется не реже чем один раз в месяц.

2.19. При обнаружении лицами, указанными в п. 4.2 настоящего Положения, нарушений в порядке обработки и защиты ПДн незамедлительно ставится в известность ответственный за защиту информации.

2.20. Ответственный за защиту информации имеет право незамедлительно приостанавливать обработку ПДн в ИСПДн до выявления причин нарушений и устранения этих причин.

2.21. Финансирование мероприятий по защите ПДн осуществляется из бюджета школы.

3. Определение уровней защищенности информационных систем персональных данных

3.1. Определение уровней защищенности ИСПДн (далее - УЗ) осуществляется с учетом категорий и объема ПДн, категорий субъектов ПДн, типа актуальных угроз безопасности ПДн в ИСПДн с целью определения требований по защите ПДн в ИСПДн.

3.2. Определение УЗ осуществляется на этапе создания ИСПДн или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

3.3. Определение УЗ осуществляется комиссией, назначаемой приказом директора школы.

3.4. Определение УЗ осуществляется в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

3.5. Определение УЗ включает в себя следующие этапы:

- сбор и анализ исходных данных по ИСПДн;
- присвоение ИСПДн соответствующего УЗ и его документальное оформление.

3.6. При определении УЗ комиссией учитываются следующие исходные данные:

- наличие актуальных угроз безопасности ПДн, связанных с недекларированными возможностями системного или прикладного программного обеспечения ИСПДн, а также не связанных с недекларированными возможностями программного обеспечения ИСПДн;
- тип информационной системы в соответствии с пунктом 5 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 N 1119;
- количество субъектов ПДн, являющихся работниками или должностными лицами школы;
- количество субъектов ПДн, не являющихся работниками или должностями лицами школы;
- иные сведения, которые могут потребоваться для определения УЗ.

3.7. Исходные данные, указанные в п. 3.7 настоящего Положения, предоставляются администратором безопасности и секретарем школы.

3.8. В случае выявления в составе ИСПДн подсистем, являющихся отдельными ИСПДн, для ИСПДн, в которую входят отдельные ИСПДн, присваивается наиболее высокий УЗ, присвоенный отдельной подсистеме. При этом наиболее высоким УЗ является первый, наиболее низким - четвертый.

3.9. Результаты определения УЗ оформляются соответствующим актом, подписанным членами комиссии. Акты хранятся у ответственного за защиту информации.

3.10. УЗ может быть пересмотрен:

- в случае изменения состава актуальных угроз безопасности ПДн в ИСПДн, типа ИСПДн и иных сведений, использованных для определения УЗ;

- по результатам мероприятий по контролю уполномоченными органами за выполнением требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

4. Обязанности и права должностных лиц

4.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, привлекаются к дисциплинарной, административной, уголовной и иной, предусмотренной законодательством Российской Федерации ответственности.

4.2. Лицами, ответственными за организацию, обеспечение и выполнение мероприятий по защите ПДн, обрабатываемых в ИСПДн, являются:

- заместитель директора школы - лицо ответственное за защиту ПДн в ИСПДн;
- администратор безопасности информационных систем;
- должностные лица и работники, допущенные к обработке ПДн в ИСПДн.

4.3. Директор школы:

- осуществляет общее руководство работами по защите ПДн в ИСПДн;
- устанавливает обязанности должностных лиц, ответственных за защиту ПДн в ИСПДн;
- утверждает положения и инструкции по организации работ по защите ПДн в ИСПДн;
- назначает лицо, ответственное за защиту ПДн в ИСПДн, администратора безопасности и лиц, допущенных к обработке ПДн в ИСПДн.

4.4. Заместитель директора по безопасности – лицо, ответственное за защиту ПДн в ИСПДн:

- определяет основные мероприятия по комплексной защите ПДн в ИСПДн;
- осуществляет методическое руководство и координацию работ по защите ПДн в ИСПДн;
- контролирует работу администратора безопасности и должностных лиц, допущенных к обработке ПДн;
- организует разработку руководящих и распорядительных документов по защите ПДн в ИСПДн;
- организует и проводит занятия по изучению документов по защите ПДн в ИСПДн;
- организует обеспечение и доведение до работников и должностных лиц действующих руководящих, организационно-распорядительных и нормативно-методических документов по защите ПДн в ИСПДн;

- готовит предложения о привлечении к проведению работ по защите ПДн в ИСПДн на договорной основе организаций, имеющих лицензию на соответствующий вид деятельности;

- готовит предложения по финансированию мероприятий по защите ПДн в ИСПДн;

- участвует в проверках состояния защиты ПДн в ИСПДн;

4.5. Администратор безопасности:

- проводит работу по выявлению возможных каналов утечки ПДн в ИСПДн;

- разрабатывает руководящие и распорядительные документы по защите ПДн в ИСПДн;

- анализирует информацию, циркулирующую в ТС и системах, определяет возможные технические каналы ее утечки в ИСПДн;

- определяет реальную опасность перехвата ПДн ТС разведки, НСД к ним, разрушения (уничтожения) и искажения, разрабатывает соответствующие меры по их защите;

- вносит предложения о приостановке работ в случае обнаружения утечки (предпосылок к утечке) ПДн из ИСПДн;

- разрабатывает предложения по дальнейшему совершенствованию СЗПДн;

- непосредственно участвует в разработке инструкций и методических рекомендаций по работе с ПДн, в том числе при ее обработке с использованием ТС;

- проводит занятия с работниками и должностными лицами по вопросам защиты ПДн при использовании ТС;

- участвует в проверках состояния защиты ПДн в ИСПДн.

- совместно заместителем директора по безопасности осуществлять администрирование и обслуживание программно-технических средств защиты ПДн в ИСПДн, следить за их работоспособностью и исправностью;

4.6. Иные лица, указанные в п. 4.2 настоящего Положения, обязаны:

- не допускать проведения работ и мероприятий, связанных с использованием ПДн, обрабатываемых в ИСПДн, без принятия необходимых мер по защите ПДн;

- строго соблюдать организационно-распорядительные документы о порядке обработки и защиты ПД в ИСПДн;

4.7. Проведение работ с ПДн допускается только при выполнении требований настоящего Положения и требований иных нормативных правовых актов по вопросам защиты ПДн.

4.8. В случае обнаружения нарушений требований данного положения работником последний обязан немедленно сообщить об этом своему заместителю директора по безопасности или администратору безопасности.

4.9. На первоначальном этапе создания ИСПДн, - приобретаются сертифицированные ТС и системы, отвечающие требованиям безопасности ПДн.

4.10. Установка, подключение и настройка ТС, в соответствии с документацией к ним и планами организации и оснащения ИСПДн, обеспечивается администратором безопасности школы.

4.11. На этапе эксплуатации приобретаются лицензионные программные продукты и операционные системы, используемые в ИСПДн.

4.12. Администратор безопасности обеспечивает установку и настройку основных программных продуктов и операционных систем на ТС, а также с СЗИ.

4.13. Администратор безопасности при эксплуатации и развертывании ИСПДн в школе проводит следующие работы:

- проводит анализ возможности решения определенных задач в ИСПДн и уточнение содержания необходимых для этого изменений в конфигурации аппаратных и программных средств;
- установку (развертывание, обновление версий) программных средств, необходимых для решения конкретных задач в ИСПДн;
- удаление (затирание) программных пакетов, необходимость в использовании которых отсутствует;
- установку (развертывание) новых ИСПДн или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач.

4.14. Администратор безопасности с привлечением специалистов из других организаций, имеющих соответствующие лицензии ФСТЭК России и ФСБ России на проведение определенных работ по вопросам защиты информации, либо с привлечением отдельных работников, обеспечивает установку и настройку сертифицированных средств защиты информации и иные мероприятия, относящиеся к защите ПДн в ИСПДн.

4.15. Эксплуатация ИСПДн осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией, предписанием на эксплуатацию ТС, а также требованиями соответствующих документов по вопросам защиты ПДн.

5. Контроль состояния защиты персональных данных

5.1. Контроль состояния защиты ПДн в ИСПДн осуществляется заместителем директора по безопасности с целью проверки выполнения нормативных документов по вопросам защиты ПДн, своевременного выявления и предотвращения утечки ПДн по техническим каналам и НСД к ним.

5.2. Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты ПДн в ИСПДн, проводится администратором безопасности.

5.3. При обнаружении нарушений обработки ПДн с использованием средств вычислительной техники заместитель директора по безопасности принимает решение о прекращении работ на рабочем месте, где обнаружены нарушения, и принимает меры по их устранению.

5.4. Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер.

6. Взаимодействие с другими организациями

6.1. Взаимодействие по вопросам защиты ПДн со сторонними организациями организуется заместителем директора школы с целью:

- обеспечения недостающими и вновь разработанными руководящими, нормативно-методическими и иными документами по вопросам защиты ПДн;
- обеспечения ТС средствами защиты;
- выполнения организационных и технических мероприятий в области защиты ПДн, на проведение которых отсутствует соответствующее разрешение (лицензия) либо отсутствуют ТС и подготовленные работники (специалисты);
- контроля эффективности проводимых мероприятий по защите ПДн.

6.2. Привлекаемая для оказания услуг в области защиты информации сторонняя организация должна иметь лицензию на соответствующий вид деятельности.

6.3. Перечень совместно выполняемых организационных и технических мероприятий в области защиты информации определяется с учетом планируемых работ по созданию (модернизации) ИСПДн

6.4. С привлекаемой организацией заключается двусторонний договор (соглашение, контракт).

Положение разработал:

Заместитель директора по безопасности

А.Б. Нестеров