МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ЦЕНТР ОБРАЗОВАНИЯ № 39

имени Героя Советского Союза Алексея Арсентьевича Рогожина»

ПРИНЯТО:

Педагогическим советом

(протокол № 1 от 29.08.2023)

УТВЕРЖДАЮ:

Директор МБОУ ЦО № 39

_____ Б.В. Лобач

«29» августа 2023 г

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ЦЕНТР ОБРАЗОВАНИЯ № 39 ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА АЛЕКСЕЯ АРСЕНТЬЕВИЧА РОГОЖИНА"

Подписано цифровой подписью: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ЦЕНТР ОБРАЗОВАНИЯ № 39 ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА АЛЕКСЕЯ АРСЕНТЬЕВИЧА РОГОЖИНА"
Дата: 2024.10.02 15:40:49 +03'00'

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее Положение о защите персональных данных (далее – Положение) разработано в соответствии: Конституцией Российской Федерации (ст. 24); Трудовым Кодекса Российской Федерации (главы 14), Федеральным законом РФ от 27.07.2006 № 149-ФЗ «Об информации, информатизации и защите информации», Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных» (с учетом последней редакции); Федеральным законом РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Уставом образовательной организации, Правилами внутреннего трудового распорядка, иных нормативно-правовых актов в области защиты персональных данных.

1.2. Настоящее Положение разработано для предупреждения нарушения доступности, целостности, достоверности и конфиденциальности персональных данных, исключения угрозы и опасности утраты персональных данных (далее – ПД) и обеспечения безопасности информации в процессе управленческой и производственной деятельности образовательного учреждения.

1.3 Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

1.4 Защита персональных данных представляет собой предупреждение нарушения доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечение безопасности информации в процессе управленческой и производственной деятельности учреждения.

1.5. Защита персональных данных от неправомерного их использования или утраты обеспечивается образовательным учреждением за счет ее средств в порядке, установленном федеральным законом.

1.6. Кроме мер защиты персональных данных, установленных законодательством, образовательная организация может вырабатывать иные меры защиты персональных данных работников, обучающихся и их родителей (законных представителей).

1.7. В целях защиты конфиденциальной информации в образовательной организации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

1.8. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, и др.

1.9. Реализация мер по защите персональных данных является ответственностью оператора, т. е. руководителя и (или) уполномоченного лица, осуществляющего сбор и обработку данных в информационной системе.

2. ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

2.2 В образовательной организации с целью предотвращения угроз любого типа определяются внутренние и внешние виды защиты ПД.

2.3 «Внутренняя защита» ПД предусматривает следующие мероприятия:

- регламентация доступа персонала к конфиденциальным сведениям, документам и базам;
- разграничение полномочий между руководителями и должностными лицами образовательной организации;
- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно - методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками учреждения;
- воспитательная и разъяснительная работа с работниками образовательной

организации по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- защита персональных данных на электронных носителях.

2.4.«Внешняя защита» ПД обеспечивается проведением следующих мероприятий:

– определение и соблюдение порядка приема, учета и контроля деятельности посетителей;

- функционирование пропускного режима образовательной организации;

- обеспечение образовательной организации техническими средствами охраны, сигнализации;

- требования к защите информации при интервьюировании и собеседованиях.

2.5. Для обеспечения безопасности ПД при их обработке в Информационных системах школы осуществляется защита:

- информации, обрабатываемой с использованием технических средств;

- информации, содержащейся на бумажной, магнитной, магнитно-оптической и иной основе (носителях).

2.6. Основные направления «Внутренней защиты» ПД определяется в зависимости об способов обработки ПД в образовательной организации.

2.7. Оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) обрабатывает персональные данные:

– без использования средств автоматизации;

- в ИСПД.

3. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1 При обработке ПД руководителем и (или) уполномоченным лицом без использования средств автоматизации в образовательной организации в целях защиты ПД принимаются следующие меры:

- ограничение числа работников (с регламентацией их должностей), которым открыт доступ к персональным данным.

Руководителем образовательной организации определяется список уполномоченных лиц, имеющих доступ к ПД и утверждается приказом;

- назначение на основании приказа руководителя образовательной организации ответственного лица, обеспечивающего исполнение организацией законодательства в рассматриваемой сфере;

- утверждение перечня документов, содержащих персональные данные;

- издание внутренних документов по защите персональных данных, осуществление контроля за их соблюдением;

- ознакомление работников с действующими нормативами в области защиты персональных данных и локальными актами; проведение систематических проверок соответствующих знаний работников, обрабатывающих персональные данные, и соблюдения ими требований нормативных документов по защите конфиденциальных сведений. Следует иметь в виду, что все сотрудники, которые имеют доступ к персональным данным других людей, должны быть ознакомлены с особенностями законодательства в области защиты персональных данных;

- рациональное размещение рабочих мест для исключения несанкционированного использования защищаемой информации;

- утверждение списка лиц, имеющих право доступа в помещения, в которых хранятся персональные данные;

- утверждение порядка уничтожения информации;

- выявление и устранение нарушений требований по защите персональных данных;

- проведение профилактической работы с сотрудниками по предупреждению разглашения ими персональных данных.

3.2 Руководитель и (или) уполномоченные лица образовательной организации, связанные с обработкой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников, учащихся и их родителей (законных представителей).

3.3 ПД при их обработке, осуществляемой неавтоматизированным способом, должны обособляться от иной информации, фиксацией их на отдельных материальных носителях ПД, в специальных разделах журналов или на полях форм (бланков).

3.4 При фиксации ПД на материальных носителях не допускается фиксация на одном материальном носителе ПД, цели обработки которых заведомо несовместимы. Для обработки различных категорий ПД, осуществляемой неавтоматизированным способом, для каждой отдельной категории ПД должен использоваться отдельный материальный носитель.

3.5 При использовании типовых форм документов, характер информации в которых предполагает иди допускает включение в них ПД, должны соблюдаться следующие условия:

3.5.1 Типовая форма или связанные с ней документы (инструкции по ее заполнению, карточки, реестры и журналы) должны содержать:

Сведения о цели обработки ПД, осуществляемой неавтоматизированным способом;

- наименование оператора;
- фамилию, имя, отчество субъекта ПД;
- источник получения ПД№
- сроки обработки ПД;
- перечень действий с ПД, которые будут совершать уполномоченное лицо;
- общее описание используемых оператором способов обработки ПД.

Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую Неавтоматизированным способом.

3.5.2. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

3.5.3. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других

зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных:

3.7. При необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

3.8. При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.9. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.10. Правила настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

3.11. Уточнение персональных данных при осуществлении их обработки неавтоматизированным способом производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3.12. Обработка персональных данных, осуществляемая неавтоматизированным способом, должна производиться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.13.Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

4. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ В ИСПДн

6.4. Основной задача при обеспечении безопасности ПД при их обработке в ИСПДн является исключение или сведение к минимуму возможное влияние или воздействие на автоматизированную систему обработки изнутри или извне, которое влечет за собой любые негативные последствия для субъектов этой информации

4.2.Основные направления обеспечение информационной безопасности

- полная защиту специальных персональных данных (национальная и расовая

принадлежность, отношение к религии, состояние здоровья и личная жизнь).

- защита биометрических данных (в том числе фотографии).

- защиту общедоступных данных, то есть тех, к которым полный и неограниченный доступ предоставлен самим человеком.

4.3. Система защиты персональных данных включает в себя организационные и технические меры, определённые с учётом актуальных угроз безопасности ПД.

В целях обеспечения безопасности ПД обрабатываемых в ИСПДн проводятся следующие мероприятия:

- обновление программного обеспечения образовательной организации, в том числе совершенствование антивирусной системы;

- функционирование всех систем защиты в полную силу;

- четкая регламентация и соблюдение условий эксплуатации и хранения информации;

- обеспечение возможности зрительного контроля за серверами и доступом к ним.

- обеспечение исправности технических средств,

- обеспечение автоматической регистрации в электронном журнале безопасности полномочий сотрудников, имеющих доступ к данным, в случае изменения этих полномочий, а также возложение ответственности за информационную безопасность на специально созданное подразделение

4.4. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты данных, нейтрализующей актуальные угрозы, определённые в соответствии с частью 5 статьи 19 Ф.З. «О персональных данных».

4.5 Работы по обеспечению безопасности ПД при их обработке в Информационных системах образовательной организации являются неотъемлемой частью работ по созданию Информационных систем.

Перечень информационных систем образовательной организации устанавливается Приказом руководителя.

4.6. Проведение классификации информационных систем ПД определено Порядком проведения классификации информационных систем ПД, утвержденных совместным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности РФ, Министерством информационных технологий и связи РФ от 13.02.2008 г. №55/86/20.

4.7. Обмен ПД при их обработке в Информационных системах образовательной организации осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических и программных средств.

4.8. Размещение Информационных систем образовательной организации, специальное оборудование и охрана помещений, в которых ведется работа с ПД, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПД и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4.9. Безопасность ПД при их обработке в Информационных системах образовательной организации обеспечивает руководитель образовательной организации и (или) уполномоченное лицо. Уполномоченное лицо и руководитель образовательной организации обязаны обеспечивать конфиденциальность персональных данных, в

соответствии с определенной в образовательной организации Политикой конфиденциальности при их обработке в информационной системе.

4.10. При обработке ПД в Информационных системах образовательной организации безопасность обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного доступа к ПД и (или) передачи их лицам, не имеющим доступ к такой информации;

- своевременным обнаружением фактов несанкционированного доступа к ПД;

- недопущением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

- возможностью незамедлительного восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- постоянным контролем за обеспечением уровня защищенности ПД.

4.11. Защита ПД, обрабатываемых в Информационных системах образовательной организации, обеспечивается за счет средств образовательной организации, в порядке установленном федеральными законами.

4.12. Доступ работников образовательной организации к ПД, обрабатываемым в Информационных системах для выполнения своих должностных обязанностей производится к соответствующим ПД на основании списка, утвержденного приказом руководителя образовательной организации.

5. ПОРЯДОК И ОСНОВНЫЕ НАПРАВЛЕНИЯ «ВНЕШНЕЙ ЗАЩИТЫ» ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Основной целью мероприятий по организации «внешней защиты» ПД является исключение или сведение к минимуму возможность доступа к ПД посторонних лиц.

5.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к учреждению, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

5.3 Основные меры «внешней защите» персональных данных в образовательной организации:

- введение пропускного режима, порядка приема и учета посетителей;

- внедрение технических средств охраны, программных средств защиты информации на электронных носителях и др.;

- обеспечение фиксации и учета ПД, переданных третьим лицам, контролирующим органам, а также при передаче ПД в другие структурные подразделения образовательной организации в соответствии с Положением о работе с персональными данными работников и Положением о работе с персональными данными учащихся и третьих лиц.

5.4. В целях соблюдения конфиденциального режима работы с персональными в образовательной организации ведется журнал учета выдачи персональных данных другим лицам, структурным подразделениям и государственным органам. В журнале учета

уполномоченным лицом регистрируются все поступающие запросы, а также ведется фиксация сведения о лице, направившем запрос, дате передачи персональных данных или факте уведомления об отказе в их предоставлении, содержание переданной информации.

6. ОБЯЗАННОСТИ ЛИЦ, ИМЕЮЩИХ ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

6.1. Ответственность за обеспечение безопасности персональных данных и надлежащий режим работы Информационных систем образовательной организации возлагается на руководителя образовательной организации.

6.2. В своей работе уполномоченные лица и руководитель образовательной организации, допущенные к обработке персональных данных в Информационных системах, должны руководствоваться требованиями федеральных законов, нормативно-правовых документов Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации, а также настоящим Положением.

6.3. В должностные инструкции работников образовательной организации, уполномоченных на обработку персональных данных в Информационных системах, должны быть внесены обязанности о необходимости выполнения требований по обеспечению безопасности обрабатываемых ими персональных данных.

6.4. Ответственный за обеспечение безопасности персональных данных в образовательной организации руководствуется в своей деятельности инструкцией ответственного за обеспечение безопасности персональных данных, обрабатываемых в Информационных системах.

6.5. При обнаружении нарушений порядка предоставления персональных данных, обрабатываемых в Информационных системах, руководитель и (или) уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям Информационных систем до выявления причин нарушений и устранения этих причин.

6.6. За нарушение норм настоящего Положения, а также федеральных законов, регламентирующих порядок обработки и обеспечения безопасности персональных данных, руководитель и (или) уполномоченные лица, допущенные к работе с персональными данными в Информационных системах, несут гражданско-правовую, административную, уголовную и дисциплинарную ответственность в соответствии с действующим законодательством.

7. ПОРЯДОК ПРИНЯТИЯ И ИЗМЕНЕНИЯ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

7.1. Положение утверждается Приказом директора образовательной организации.

7.2. Внесение изменений и дополнений в настоящее Положение осуществляется в порядке принятия основного документа.

7.3. Неотъемлемой часть настоящего Положения являются:

1) Приложение № 1 – Лист ознакомления с Положением о защите персональных данных.