УТВЕРЖДЕНО
приказом директора МБОУ Гимназия №4 от 27.04.2016 № 93/1

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке МБОУ Гимназия № 4

Содержание

1. Общие положения

1.1. Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке МБОУ Гимназия № 4 (далее в тексте – Положение) принято в целях обеспечения защиты прав и свободы категорий субъектов при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, в МБОУ Гимназия 4 (далее в тексте – гимназия).

1.2. Правовое основание обработки персональных данных осуществляется на основе: Конвенции Совета Европы о защите физических лиц при автоматизированной обработке данных от 28.01.1981, Федерального закона от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке данных», Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федеральных законов от Федеральный закон от 07.02.2017 № 13-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. от 01.07.2017 № 148-ФЗ), от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе» (с изм. на 03.07.2016 № 305-ФЗ), постановлениями Правительства РФ от 15.09.2008 № 687 «Об утверждении

Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 27.11.2006 № 719 «Об утверждении Положения о воинском учете» (ред. от 21.04.2016), постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. на 21.07.2014 № 242-ФЗ), постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», постановления Минтруда РФ от 10.10.2003 № 69 «Об утверждении инструкции по заполнению трудовых книжек», Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации (с доп.), постановления Правительства РФ от 16.04.2003 № 225 «О трудовых книжках» (в ред. от 25.03.2013 № 257), приказа Роскомнадзора от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных», устава гимназии.

1.3. Персональные данные относятся к категории конфиденциальной информации.

1.4. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.
1.5. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

1.6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

1.7. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.8. Настоящее Положение утверждается приказом директора гимназии и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

2. Цель, категории субъектов, категории персональных данных

2.1. Целью обработки персональных данных является осуществление образовательной деятельности, кадрового обеспечения деятельности учреждения, ведения бухгалтерского учета в соответствии с законодательством РФ.

2.2. Категории субъектов, персональные данные которых обрабатываются – работники учреждения, состоящие в трудовых (договорных) отношениях с учреждением; юридические и физические лица, состоящие в трудовых (договорных) отношениях с учреждением; обучающиеся учреждения и их родители (законные представители), отношения с которыми основываются во исполнение Федерального закона «Об образовании в Российской Федерации»; дети дошкольного возраста, дети, не являющиеся обучающимися учреждения и их родители (законные представители), а также взрослые люди, отношения с которыми выстраиваются для предоставления платных дополнительных услуг.

2.3. Категории персональных данных: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; семейное положение; социальное положение; имущественное положение; образование; профессия; доходы; национальная принадлежность; состояние здоровья; биометрические персональные данные: фотографии, видеофрагменты; биографические данные; сведения о стаже; сведения о составе семьи; паспортные данные; данные свидетельства о рождении; данные медицинского полиса; данные медицинской книжки, данные паспорта здоровья; сведения о воинском учете; сведения о заработной плате; сведения о социальных льготах; данные сведений об образовании; квалификация и специальность; квалификационная категория; занимаемая должность; судимость; адрес места жительства и мест регистрации; домашний, сотовый и рабочий телефоны; адрес личной электронной почты; место работы или учебы членов семьи и родственников; характер взаимоотношений в семье; содержание трудового договора; состав декларируемых сведений о наличии материальных ценностей; содержание декларации, подаваемой в налоговую инспекцию; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников; основания к приказам по личному составу; дела, содержащие материалы по повышению квалификации и переподготовке; аттестация работников; данные служебного расследования; копии отчетов, направляемые в контролирующие и надзорные органы, другие органы, с которыми учреждение связано при выполнении осуществлении образовательной и трудовой деятельности; подлинники и копии приказов по обучающимся; принадлежность к классу; данные оценки успеваемости обучающихся в течение года; данные о результатах промежуточной и итоговой аттестации обучающихся; данные о результатах конкурсных мероприятий учащихся и работников; дата поступления в гимназию, дата и причина отчисления из гимназии, перевод из класса в класс; знание иностранных языков; группа здоровья, психолого-педагогическая и логопедическая характеристика, которые относятся к вопросу оптимальной организации образовательного процесса; сертификат дополнительного образования; форма получения образования и форма обучения; программа обучения; предметы для ОГЭ и ЕГЭ, тип документа для ОГЭ и ЕГЭ; данные о результатах конкурсных мероприятий (олимпиад, конференций, спортивных соревнований, творческих конкурсов, интеллектуальных игр, конкурсов профессионального мастерства и т.п.) учащихся и работников; документы о составе семьи; документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний и т.п.); документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.); данные свидетельства о заключении брака; данные полиса обязательного медицинского образования; данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ; данные

страхового свидетельства государственного пенсионного страхования; данные полиса обязательного медицинского страхования; данные дипломов об образовании.

3. Права и обязанности оператора персональных данных

3.1. В целях обеспечения прав и свобод человека и гражданина оператор и при обработке персональных данных обязан соблюдать следующие общие требования:

3.1.2. Обработка персональных данных в гимназии осуществляется в соответствии с целями п. 2.1.

3.1.3. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом, Федеральным законом «Об образовании в Российской Федерации» и иной нормативной документацией федерального уровня.

3.1.4. Все персональные данные следует получать у субъекта персональных данных. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

3.1.5. Оператор не имеет права получать и обрабатывать персональные данные о политических, религиозных и иных убеждениях субъекта.

3.1.6. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в установленном порядке.

3.1.7. Работники должны быть ознакомлены, с документами гимназии, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.

4. Права и обязанности субъекта персональных данных

4.1. Обязанности субъекта:

- передавать оператору или его полномочному должностному лицу комплекс достоверных, документированных персональных данных, состав которых установлен ФЗ «О персональных данных» для исполнения оператором трудовых отношений и ведения образовательной деятельности;
- своевременно сообщать оператору об изменении своих персональных данных.

4.2. Права субъекта:

- требовать изменения, уничтожения или блокирования неверных или неполных персональных данных;
- на свободный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- получать от оператора персональных данных информацию о
- правовых основаниях и целях обработки персональных данных;
- целях и применяемых способах обработки персональных данных;
- наименовании и месте нахождения оператора;
- сведениях о третьих лицах (за исключением работников МБОУ Гимназия № 4), которые имеют доступ к персональным данным или которые могут быть раскрыты на основании договора или на основании нормативных правовых актов;

- обрабатываемых персональных данных, источнике их получения, если иной порядок предоставления таких данных не предусмотрен нормативными правовыми актами;
- сроках обработки и сроках хранения персональных данных;
- порядке осуществления субъектом персональных данных своих прав;
- о трансграничной передаче или не осуществлении ее;
- иных сведениях, предусмотренных нормативными правовыми актами;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных; - на сохранение и защиту своей личной и семейной тайны.

5. Рассмотрение запросов субъектов персональных данных или их законных представителей

5.1. МБОУ гимназия № 4 обязано безвозмездно предоставлять субъекту персональных данных или ему законному представителю возможность ознакомления с персональными данными, относящимся к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Сведения, установленные в п. 4.2. настоящей Политики, предоставляются МАОУ Гимназия № 10 субъекту персональных данных в доступной форме или в унифицируемой запрашиваемой форме и не должны содержать персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Основанием для предоставления сведений, установленных в п. 4.2. настоящей Политики, является обращение либо поручение субъекта персональных данных или его законного представителя, содержащего следующие позиции:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдаче и выдававшем его органе;
- документ, удостоверяющий полномочия предоставления интересов субъекта персональных данных;
- сведения, подтверждающие факт персональных данных МБОУ Гимназия № 4; - подпись субъекта персональных данных или его законного представителя.

Запрос может быть направлен в письменной форме, форме электронного документа, подписанного электронной подписью.

6. Перечень действий с персональными данными

6.1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом или другими федеральными законами.

На документах, содержащих персональные данные, соответствующий гриф ограничения не ставится в виду их массовости и постоянного процесса уточнения. При этом в гимназии соблюдается достаточный комплекс мер по защите персональных данных, содержащийся в Инструкции о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

В гимназии осуществляется смешанная обработка персональных данных. Информация может передаваться по локальной сети гимназии с соблюдением прав граждан на сохранность персональных данных (ограниченный доступ через логины и пароли).

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая бор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Основные понятия действий с персональными данными:

- использование - действия (операции) с персональными данными, совершаемые должностным лицом школы в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников (учащихся) либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- передача (распространение, предоставление, доступ) - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц;
- обезличивание - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- блокирование - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- уничтожение - 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.

6.2. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники, непосредственно использующие их в служебных целях, в пределах исполнения своих служебных обязанностей:

- административно-управленческого персонала; - основного персонала;
- вспомогательного персонала.

6.3. При передаче персональных данных оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные

данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

6.4. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.5. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные (материальные, неавтоматизированные) носители, так и на электронные (автоматизированные) носители информации.

6.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

6.8. Создание персональных данных обучающегося и его родителей (или законных представителей).

Документы, содержащие персональные данные обучающегося и его родителей (или законных представителей), создаются путем:

а) предъявления оригиналов (паспорта или свидетельства о рождении обучающегося; документа, выданного медицинским учреждением в соответствии с действующим законодательством; документа, удостоверяющего личность родителей (законных представителей) или заявителя);

б) внесения сведений в учетные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (выписка текущих оценок по всем предметам и личное дело обучающегося, документ об образовании, сведения о текущей успеваемости и результатах промежуточной аттестации).

6.9. Создание персональных данных работника.

Документы, содержащие персональные данные работника, создаются путем:

а) предъявления оригиналов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство);

б) внесения сведений в учетные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учѐту кадров, автобиография, медицинское заключение).

6.10. В случае выявления работником МБОУ Гимназия №4 неправомерной обработки персональных данных или выявления неточных персональных данных при обращении субъекта или его законного представителя либо по запросу уполномоченного органа по защите прав субъектов персональных данных, ставится в известность ответственный за организацию обработки персональных данных, который инициирует блокирование персональных данных, относящихся к этому субъекту персональных данных.

В случаях, если отсутствует возможность уничтожения персональных данных, МБОУ Гимназия № 4 осуществляет блокирование таких персональных данных и обеспечивает уничтожение в срок не более чем шесть месяцев.

6.11. Обезличивание персональных данных проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено нормативными правовыми актами.

Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение/ понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улица, дома и квартиры, а может быть указан только город); - деление сведений на части; - другие способы.

Способом обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

В соответствии с Положением о разграничении прав доступа к обрабатываемым персональным данным обезличивание могут производить работники, занимающие следующие должности: директор, секретарь руководителя, зам. директора (по УВР, ВР), старший учитель, гл. специалист МиИП, главный бухгалтер, бухгалтер.

Требования к соблюдению конфиденциальности при работе с обезличенными данными предъявляются те же что и при работе с не обезличенными персональными данными: не подлежат разглашению и нарушению конфиденциальности, соблюдается парольная и антивирусная защита, правила доступа в помещения (см. - Требования к оборудованию помещений, размещению технических средств, используемых для обработки персональных данных, и сейфов для хранения документов, связанных с обработкой персональных данных, а также к допуску к ним ответственных лиц») и т.п.

6.12. Персональные данные подлежат уничтожению или обезличиванию в следующих случаях и в указанные сроки в соответствии со статьями ФЗ «О персональных данных» и не подлежащих архивному хранению:

- по достижении целей обработки персональных данных – в 30-дневный срок;
- в случае утраты необходимости в достижении целей обработки персональных данных – в 30-дневный срок;
- в случае отзыва субъектом персональных данных согласия на обработку персональных данных – в 30-дневный срок, если иной срок не предусмотрен договором или соглашением между МАОУ Гимназия № 10 и субъектом персональных данных, либо если МАОУ Гимназия № 10 не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных 152-ФЗ или другими нормативными правовыми актами;
- персональные данные являются незаконно полученными – в 10-дневный срок;
- персональные данные являются неполными, устаревшими, неточными (при условии, что уточнение персональных данных невозможно) – в 10-дневный срок; - персональные данные не являются необходимыми для заявленной цели обработки – в 10-дневный срок.

Процесс уничтожения персональных данных при достижении целей их обработки либо в случае утраты необходимости в достижении этих целей инициирует оператор информационной системы персональных данных (см. - Положение о разграничении прав доступа к обрабатываемым персональным данным), в которой эти персональные данные обрабатываются. Оператор согласовывает уничтожение с ответственным за организацию обработки персональных данных в устной форме.

В остальных случаях, в том числе при отзыве субъектом персональных данных согласия на обработку своих персональных данных, процесс уничтожения персональных данных инициируется ответственным за организацию обработки персональных данных.

Оператор информационной системы персональных данных после согласования с ответственным за организацию обработки персональных данных в случае с бумажными носителями персональных данных производит уничтожение персональных данных путем сожжения, разрывания (до момента невозможности идентификации персональных данных) или закрашивания, в случае с персональными данными, содержащимися на электронных носителях – путем удаления файла, документа, папки, записи в базах данных.

7. Доступ к персональным данным субъекта

7.1. Внутренний доступ.

Доступ к персональным данным субъекта имеют должностные лица, непосредственно использующие их в служебных целях, в пределах исполнения своих должностных обязанностей и непосредственно субъект персональных данных (см. - Перечень должностей работников, осуществляющих обработку персональных данных).

Другие работники имеют доступ к персональным данным субъекта только с письменного согласия самого субъекта, носителя данных.

7.2. Внешний доступ.

7.2.1. К числу массовых потребителей персональных данных вне общеобразовательного учреждения относятся государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных, региональных и российских органов управления.

7.2.2. Надзорно-контрольные органы имеют доступ к информации только в пределах своей компетенции.

7.2.3. Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

7.2.4. Другие организации.

Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

7.2.5. Родственники и члены семей.

Персональные данные могут быть предоставлены родственникам или членам семьи субъекта только с письменного разрешения самого субъекта.

7.3. Доступ к персональным данным обучающегося.

Личные дела обучающихся хранятся в запертом металлическом сейфе. Доступ к сейфу и персональному компьютеру, содержащему информацию с персональными данными обучающегося строго ограничен кругом лиц, внесенных в Положение о разграничении прав доступа к обрабатываемым персональным данным.

Доступ к персональным данным обучающихся имеют работники, должности которых включены в Перечень должностей, осуществляющих обработку персональных данных, и непосредственно использующие их в служебных целях, в пределах исполнения своих должностных обязанностей.

Ответственные лица имеют право получать только те персональные данные обучающегося и его родителей (законных представителей), которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных обучающегося, определяются трудовыми договорами и должностными инструкциями.

Персональные данные обучающегося предоставляются родителям (законным представителям) данного обучающегося на основании письменного заявления родителя (законного представителя). Не имеет права получать информацию об обучающемся родитель, лишенный или ограниченный в родительских правах на основании вступившего в законную силу постановления суда.

7.4. Доступ к персональным данным работника.

Трудовая книжка, документы воинского учѐта, карточка формы Т-2, приказы по личному составу хранятся в запертом металлическом сейфе.

Доступ к сейфу, персональному компьютеру, содержащему информацию с персональными данными работников строго ограничен кругом лиц, внесенных в Положение о разграничении прав доступа к обрабатываемым персональным данным.

Доступ к персональным данным работников имеют работники, должности которых включены в Перечень должностей, осуществляющих обработку персональных данных, и непосредственно использующие их в служебных целях, в пределах исполнения своих должностных обязанностей.

Ответственные лица имеют право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц. Все остальные работники имеют право на полную информацию только об их персональных данных и обработке этих данных.

8. Защита персональных данных

8.1. 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.

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.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

8.2. Внутренняя защита.

В МБОУ Гимназия № 4 в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуется проведение периодических проверок условий обработки персональных данных, регламентируемое в локальном нормативном акте «Порядок проведения внутреннего контроля».

Регламентация доступа персонала к конфиденциальным сведениям, документам и базе данных входит в число основных направлений организационной защиты информации в гимназии и предназначена для разграничения полномочий сотрудников. Для защиты персональных данных в гимназии должны соблюдаться следующие меры:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют выполнение работы с персональными данными;
- строгое избирательное и обоснованное распределение документов и информации между ответственными работниками;
- рациональное размещение рабочих мест работников, при котором исключается 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;
- воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- хранение информации на бумажных носителях в сейфах;
- логины и пароли в информационных системах;
- обеспечение защиты внутренней локальной сети гимназии.

8.3. Внешняя защита.

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

Для защиты персональных данных от внешней угрозы в гимназии должны соблюдаться ряд мер:

- порядок контроля за деятельностью посетителей (камеры наблюдения, охранная служба, дежурные администраторы, учителя и классы);
- порядок охраны территории, здания, помещений;
- требования к защите информации от постороннего доступа и просмотра;
- установка антивирусной защиты;
- внешняя защита на сервер гимназии (файрвол).

8.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут ответственность в соответствии с действующим законодательством.

9. Парольная защита при обработке персональных данных и иной конфиденциальной информации

9.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей и контроль за действиями пользователей при работе с паролями возлагается на работников технической службы ИВТ: администратора вычислительной сети и инженера (по обслуживанию ИВТ).

Учащийся осуществляет вход в локальную систему под индивидуальным логином и паролем класса, внесенным в Журнал учета логинов, присвоенных работнику и классам, имеющим доступ к информационной системе.

Работник осуществляет вход в локальную сеть под индивидуальным логином и паролем, внесенным в Журнал учета логинов, присвоенных работнику и классам, имеющим доступ к информационной системе. Работником технической службы ИВТ выдается одноразовый пароль для входа в систему, пользователь при первичном заходе устанавливает свой пароль.

Доступ обучающихся и их родителей (законных представителей), работников гимназии (далее в тексте – пользователи) к сервисам информационных систем «Дневник.ру» и/или «Электронная школа» обеспечивается после их регистрации в установленном порядке, регламентированном в локальном нормативном акте «Положение о ведении журнала, обеспечивающего учет выполнения образовательной программы, в электронном виде» и внесенным в Журнал учета логинов для регистрации в информационных системах «Дневник.ру» и/ или «Электронная школа».

9.2. Основные правила информационной безопасности.

Пароль - это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий.

Наиболее надежный пароль содержит буквы разных регистров, цифры и специальные символы, не содержит логин, содержит не менее 8 символов. В числе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы, пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

Нельзя оставлять логин и пароль в общедоступных местах.

Нельзя передавать пароль другим лицам.

Нельзя разрешать программному обеспечению «запоминать» логин и пароль в общедоступных местах: при включении функции сохранения пароля интернет-браузер запомнит данные пользователя для входа, и воспользоваться профилем сможет любой желающий, продолживший работать за общедоступным компьютером.

Из учетной записи необходимо выходить сразу после завершения работы.

Необходимо подтверждать e-mail и номер телефона: подтвержденный e-mail необходим для защиты страницы. При попытке смены пароля на почту пользователя приходит соответствующее уведомление, и другое лицо не сможет осуществить взлом. Также с его помощью восстанавливается доступ в систему, если пользователь забывает свой пароль.

9.3. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на работников технической службы ИВТ.

Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих работников технической службы ИВТ с паролями других работников.

Смена личного пароля или удаление учетной записи пользователя в случае компрометации личного пароля пользователя или прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться работниками технической службы ИВТ немедленно после окончания последнего сеанса работы данного пользователя с системой.

Полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) работника технической службы, которому по роду деятельности были предоставлены полномочия по управлению парольной защитой.

Системный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на работников технической службы ИВТ.

10. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

10.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

10.2. Директор, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

10.3. Каждый работник гимназии, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

10.4. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации по персональным данным несут ответственность в соответствии с действующим законодательством.