

Утверждаю
Директор
МБОУ Комсомольской СОШ



Е.В. Рамхин
(подпись, инициалы, фамилия)

«30» января 2013 г.

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

1.1. Настоящее Положение разработано в целях защиты персональных данных, обрабатываемых в информационных системах персональных данных Муниципального бюджетного общеобразовательного учреждения Комсомольской средней общеобразовательной школы Первомайского района (МБОУ Комсомольской СОШ), от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Положение определяет обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.3. Положение разработано на основании ст.24 Конституции РФ, Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., Постановления Правительства Российской Федерации от 17.11.2007г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений.

1.4. Настоящее Положение утверждается директором МБОУ Комсомольской СОШ

1.5. Изменения в Положение могут быть внесены в установленном действующим законодательством порядке.

1.6. В настоящем Положении используются следующие основные понятия:

1.6.1. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных) – работнику, абитуриенту, обучающемуся, выпускнику;

1.6.2. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

1.6.3. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

1.6.4. Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

1.6.5. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

1.6.6. Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

1.6.7. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных

достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

3.7. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями *МБОУ Комсомольской СОШ*.

3.8. Персональные данные могут храниться в бумажном и(или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных.

3.9. Перечень структурных подразделений и (или) отдельных должностей, имеющих право на обработку персональных данных предоставляется работникам структурных подразделений и(или) должностным лицам, определенным отдельными Приказами, распорядительными документами и иными письменными указаниями уполномоченных сотрудников *МБОУ Комсомольской СОШ*.

3.10. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Оператора

4. Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных

4.1. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

4.1.1. На получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;

4.1.2. Требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

4.1.3. На получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

4.1.4. На обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

4.1.5. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4.2. Обязанности Оператора при сборе персональных данных.

4.2.1. Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.2.2. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

4.2.3. В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения.

4.2.4. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные.

4.2.5. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

6.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

6.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) 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;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

6.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

6.7. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению №3 к настоящему Положению.

К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

6.8. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

а) 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;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим

перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. 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 невазимо связанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

7.4. Непрерывность защиты персональных данных

Защита персональных данных – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы персональных данных.

Информационные системы персональных данных должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационных систем персональных данных в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

7.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите информационных систем персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем персональных данных в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

7.6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем персональных данных и их системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

7.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

7.8. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

8. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности информационных систем персональных данных подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в плане мероприятий по обеспечению защиты персональных данных.

8.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

8.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

8.3. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования информационных систем персональных данных, использование ресурсов информационных систем персональных данных, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с информационными системами персональных данных таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, принимаемых на высшем управленческом уровне - сформировать политику информационной безопасности персональных данных (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация политики информационной безопасности персональных данных в информационных системах персональных данных состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность рассматриваемых в целом. Эти решения закрепляются в локальных актах Организации. Примером таких решений могут быть:

в данном помещении в связи с выполнением своих должностных обязанностей. Доступ в помещение в неуточное время или в выходные и праздничные дни осуществляется с письменного разрешения заместителя директора по АХЧ МБОУ Комсомольской СОШ.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключая нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

8.5. Аппаратно-программные средства защиты ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных и информационных системах по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационных систем персональных данных;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам информационных систем персональных данных Администрации;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- обязательное резервирование всей информации, имеющей конфиденциальный характер;
- дублирование информации с использованием различных физических и аппаратных носителей;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты персональных данных.

Успешное применение технических средств защиты на основании представленных выше принципов предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

обеспечена физическая целостность всех компонент информационных систем персональных данных;

каждый сотрудник (пользователь) или группа пользователей информационных систем персональных данных имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

все изменения конфигурации технических и программных средств информационных систем персональных данных производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства МБОУ Комсомольской СОШ;

сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних лиц (специальных помещениях, шкафах, и т.п.).

специалистами МБОУ Комсомольской СОШ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

С целью поддержания установленного уровня защищенности информации, применяемые меры обеспечения безопасности должны регулярно пересматриваться и приводиться в соответствие с новыми требованиями.