Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа № 10»
г.Выборг

ПРИКАЗ

04.09.2017 г. № 265

О создании системы защиты
персональныхданных

В целях организации работы по защите персональных данных в МБОУ «СОШ № 10» (далее – ОО – образовательная организация), с учетом требований закона от 27.07.2006 №152- ФЗ «О персональных данных» и НМД Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утверждённых приказом Гостехкомиссии России от 30 августа 2002 года №282 и методических документов ФСТЭК России

.

ПРИКАЗЫВАЮ:

1. Назначить секретаря школы Попову А.В. ответственным за обеспечение защиты персональных данных в МБОУ «СОШ № 10».

2. Секретарю Поповой А.В.:

2.1. Осуществлять режим защиты персональных данных на основании Положения об обработке персональных данных работников.

2.2. Провести внутреннюю проверку защиты персональных данных в срок до 26.09.2017 г.

2.3. О результатах внутренней проверки информировать директора школы до 03.10.2017 г.

3. Утвердить:

3.1. Перечень сведений, составляющих персональные данные в ОО (Приложение 1).

3.2. Инструкцию пользователя информационной системы персональных данных (Приложение 2).

3.3. Разрешительную систему доступа к персональным данным МБОУ «СОШ № 10» (Приложение 3).

3.4. План мероприятий по обеспечению защиты персональных данных.

3.5. План внутренних проверок защиты персональных данных.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор О.С. Лобанкова

С приказом ознакомлены:

Приложение 1
к приказу от 04.09.2017 г. №265

Перечень сведений, составляющих персональные данные в ОО

К персональным данным работника, получаемым работодателем и подлежащим хранению у работодателя в порядке, предусмотренном действующим законодательством и Положением о защите и работе с персональными данными работников (утв. приказом от 31.08.2016 г. № 249), относятся следующие сведения, содержащиеся в личных делах работников:

– паспортные данные работника;

– ИНН;

– копия страхового свидетельства государственного пенсионного страхования;

– копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

– копия документа об образовании, квалификации или наличии специальных знаний;

– анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в том числе – автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);

– документы о возрасте малолетних детей и месте их обучения;

– документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);

– документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);

– медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров;

– трудовой договор;

– копии приказов о приеме, переводах, увольнении;

– личная карточка по форме Т-2;

– заявления, объяснительные и служебные записки работника;

– документы о прохождении работником аттестации, повышения квалификации;

– справки, содержащие информацию о наличии или отсутствии судимости.

К персональным данным обучающихся, получаемым ОО и подлежащим хранению в порядке, предусмотренном действующим законодательством, относятся следующие сведения, содержащиеся в личных делах обучающихся:

– документы, удостоверяющие личность обучающегося (копии свидетельств о рождении или паспорта);

– документы о месте проживания;

– документы о составе семьи;

– паспортные данные родителей (законных представителей) обучающегося;

– документы о получении образования, необходимого для поступления в соответствующий класс (личное дело, справка с предыдущего места учебы и т.п.);

– документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний, медицинское заключение об отсутствии противопоказаний для обучения в образовательном учреждении конкретного вида и типа, о возможности изучения предметов, представляющих повышенную опасность для здоровья и т.п.);

– документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители- инвалиды, неполная семья, ребенок-сирота и т.п.).

Приложение 2
к приказу от 04.09.2017 г. № 265

Инструкция пользователя информационной системы персональных данных

1. Общие положения

1.1.Настоящая инструкция разработана на основании:
-Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
-Положения «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации №781 от 17 ноября 2007г.;
-Приказа №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного ФСТЭК России от 05.02.2010 г.;
- Постановлением Правительства Российской Федерации от 17 ноября 2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Данная инструкция определяет общие обязанности, права и ответственность пользователя информационной автоматизированной и неавтоматизированной системы персональных данных (далее – ИСПДн) МБОУ «СОШ № 10» по обеспечению информационной безопасности при работе со сведениями конфиденциального характера.
1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник МБОУ «СОШ № 10», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной и неавтоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн (в том числе, находящихся на неэлектронных носителях).
1.4. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.
1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся под подпись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

2. Обязанности пользователя

2.1. При выполнении работ в ИСПДн (при автоматизированной и неавтоматизированной обработке) Пользователь обязан:
- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными, техническими и нетехническими средствами ИСПДн, правила работы и порядок регистрации в ИСПДн, доступа к информационным ресурсам ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (АРМ);
- хранить в тайне свои идентификационные данные (имена, пароли и т.д.);
- осуществлять вход в ИСПДн только под своими идентификационными данными; передавать для хранения установленным порядком свое индивидуальное устройство идентификации, личную ключевую дискету и другие реквизиты разграничения доступа, только руководителю ОО или ответственному за защиту персональных данных в ОО;

- работать в ИСПДн только в разрешенный период времени;
- предоставлять свое АРМ администрации школы для контроля;
- ставить в известность ответственного за защиту персональных данных в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ;
- сообщать руководителю своего подразделения обо всех проблемах, связанных с эксплуатацией ИСПДн.

2.2. Пользователю категорически ЗАПРЕЩАЕТСЯ:
- использовать компоненты программного и аппаратного обеспечения ИСПДн (в том числе, находящихся на неэлектронных носителях) в неслужебных целях;
- самовольно вносить какие-либо изменения, осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию на неучтенных носителях информации в том числе для временного хранения;
- оставлять включенное без присмотра свое АРМ, не активизировав временную блокировку экрана и клавиатуры;
- передавать, оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);
- разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;

3. Права пользователя

3.1. Пользователь имеет право:
- присутствовать при работах по внесению изменений в аппаратно- программную конфигурацию закрепленного за ним АРМ;
- участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными;
- своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей;

4. Ответственность пользователя

4.1. Пользователь несет персональную ответственность за: ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, и целостность установленного программного обеспечения. разглашение сведений, отнесенных к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы; нарушение функционирования ИСПДн, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

4.2. Пользователи, виновные в нарушениях несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами 3. Способы неправомерного доступа к компьютерной информации могут быть самыми различными, например, представление фиктивных документов на право доступа к информации, изменение кода или адреса технического устройства, нарушение средств или системы защиты информации, кража носителя информации.

Приложение 3
к приказу от 04.09.2017 г. № 265

Разрешительная система доступа к персональным данным МБОУ «СОШ № 10»

Перед предоставлением сотруднику доступа к информационным ресурсам ОО, содержащим персональные данные, необходимо ознакомить сотрудника под подпись со следующими документами:

- Перечень персональных данных ОО;

- Инструкция по обеспечению безопасности обрабатываемых персональных данных;

- Инструкции пользователей информационных систем персональных данных (для всех ИСПДн, используемых в ОО).

2. На основании решения директора школы (в случае необходимости) и заместителей директора осуществляется допуск пользователя к персональным данным, в объеме, необходимом для выполнения им своих функциональных обязанностей.

3. Предоставление пользователям доступа к персональным данным МБОУ «СОШ № 10» осуществляется по приказу директора школы для выполнения служебных обязанностей.

4. Прекращение предоставления доступа пользователям к персональным данным ОО в случае увольнения сотрудника.

5. Контроль правомерности предоставления доступа пользователей к информационным ресурсам возлагается на ответственного за защиту персональных данных МБОУ «СОШ № 10».

6. Сотрудники МБОУ «СОШ № 10», допущенные к работе с персональными данными, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность за разглашение персональных данных в соответствии с законодательством Российской Федерации.

Приложение 4
к приказу от 04.09.2017 г. № 265

План мероприятий по обеспечению безопасности персональных данных

Мероприятие	Периодичность	Исполнитель/ Ответственный
Организационные мероприятия		
Определение обрабатываемых персональных данных и объектов защиты	Ежегодно (начало учебного года)	Попова А.В.
Определение и корректировка перечня информационной системы персональных данных	Ежегодно (начало учебного года)	Попова А.В.
Определение круга лиц участвующих в обработке персональных данных	Ежегодно (в теч. года)	Лобанкова О.С.
Определение ответственности лиц участвующих в обработке	Ежегодно (в теч. года)	Лобанкова О.С.
Определение прав разграничения доступа пользователей информационной системы персональных данных, необходимых для выполнения должностных обязанностей	Ежегодно (начало учебного года)	Лобанкова О.С.
Назначение ответственного за обеспечение защиты персональных данных в МБОУ «СОШ № 10»	Ежегодно (начало учебного года)	Лобанкова О.С.
Введение режима защиты персональных данных в МБОУ «СОШ № 10»	Ежегодно (начало учебного года)	Лобанкова О.С.
Организация информирования и обучения сотрудников о порядке обработки персональных данных	Ежегодно (начало учебного года)	Попова А.В.
Контролирующие мероприятия		
Контроль над соблюдением режима обработки персональных данных	Ежедневно	Попова А.В.
Контроль над соблюдением режима защиты	Ежедневно	Попова А.В.
Контроль за обновлениями программного обеспечения на всех элементах ИСПДн	Раз в полгода	Попова А.В., Черепова А.В., Дегтярёва Т.В.

Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Кристианс Е.В.

Приложение 5

к приказу от 04.09.2017 г. № 265

План внутренних проверок защиты персональных данных

Мероприятие	Периодичность	Исполнитель
Контроль над соблюдением режима обработки персональных данных	Еженедельно	Попова А.В.
Контроль над соблюдением режима защиты	Ежедневно	Попова А.В.
Контроль над выполнением антивирусной защиты	Ежемесячно	Патрикеев В.Б.
Контроль над соблюдением режима защиты при подключении к сетям общего пользования	Еженедельно	Патрикеев В.Б.
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты персональных данных	Ежегодно	Попова А.В.
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	Попова А.В., Черепова А.В., Дегтярёва Т.В.
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	Попова А.В.
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Кристианс Е.В.