УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

Инструкция
по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Настоящая инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской (далее - ИСПДн).
2. Порядок допуска работника к работе с персональными данными:
— утверждение приказом о допуске к обработке персональных данных перечня должностей работников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (далее - Перечень);
— прохождение первичного инструктажа, включающего ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными, согласно Инструкции по проведению инструктажа лиц, допущенных к работе с персональными данными с внесением соответствующей информации в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными в ИСПДН;
— внесение записи в Журнал учёта прав доступа к ИСПДн.
3. Допуск работника к персональным данным прекращается:
— в случае обнаружения нарушений порядка обработки персональных данных до выяснения и устранения причин нарушений;
— в случае увольнения сотрудника с момента подписания приказа об увольнении;
— при изменении его служебных обязанностей с момента утверждения нового Перечня.

Ознакомлены:

Алексеева Д.С.
Андрющенко И.М.
Близнюк Н.А.
Белан В.О.
Будлянская Ю.В.
Ваганова В.Б.
Власенко О.А.
Волошенко А.С.
Гаврищака И.Н.
Галицына Н.Д.
Гендель Т.Г.
Дурасова А.Н.
Ельникова Е.В.
Жогло Т.Б.
Заика А.Н.
Залозний С.А.
Захарина Н.Н.
Иваненко Р.А.
Кадырова Л.В.
Кандаурова Н.Г.
Кашина О.А.
Кисиль О.Ю.
Коваль Н.В.
Коломиец С.В.
Коломиец Г.Г.
Кулинич С.П.
Куцевол О.И.
Лагун В.Н.
Ларина В.А.
Левченко Е.Н.
Матвиенко Т.В.
Мельникова Ю.Ю.
Метченко Г.Н.
Милосердова В.А.
Михайленко Т.В.

Мосиенко Е.В.
Никитина Т.Н.
Оверченко И.А.
Олейник М.Н.
Пасюта Н.В.
Панченко Л.В.
Подпорина Е.Ю.
Подсекина И.И.
Пономарева А.С.
Потурнак Е.Ю.
Пташенко Л.Б.
Ровная Е.В
Ровная Е.В. (л)
Рой Ю.С.
Рыжая В.С.
Савранская Н.П.
Семёнова В.В.
Скворцова Т.И.
Слесаренко Т.Ю.
Стороженко Е.В.
Стрюк О.В.
Терешок О.Г.
Тертица И.Б.
Тололина Н.Г.
Уткина Г.А.
Филобок Е.И.
Фоменко Е.В.
Ханина Н.В.
Цапко Г.А.
Черемскина Л.П.
Чёрная Т.Я.
Шевцова К.А.
Шелуха Ю.В.
Швидченко М.И.
Шупенко Е.А.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

Инструкция
по проведению внутреннего контроля
соответствия обработки персональных данных требованиям
к защите персональных данных в муниципальном автономном
общеобразовательном учреждении средней общеобразовательной школе
№ 2 имени Ивана Михайловича Суворова станицы Павловской

1. Общие положения

1.1. Настоящая «Инструкция по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» (далее — Инструкция) определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской (далее — Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. Инструкцию обязаны выполнять все работники Оператора, допущенные к обработке персональных данных «Приказом о допуске к обработке персональных данных».

2. Порядок проведения внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Оператор организует проведение периодических проверок условий обработки персональных данных.

2.2. Внутренний контроль проводит ответственный за организацию обработки персональных данных (далее — Ответственный) либо комиссия по персональным данным, назначенная Оператором.

2.3. Внутренний контроль осуществляется не реже 1 раза в год. При необходимости контроль может проводиться чаще в соответствии с поручением Оператора.

2.4. Ответственный либо комиссия проводит внутренний контроль непосредственно на месте обработки персональных данных, опрашивает работников, осуществляющих обработку персональных данных, осматривает рабочие места. Все работники обязаны по запросу контролирующих предъявить все материалы и документы, числящиеся за ними, дать устные или письменные объяснения по существу заданных вопросов.

2.5. По результатам проверки составляется Акт контроля соответствия обработки персональных данных по форме.

2.6. При выявлении нарушений в ходе проверки Ответственным либо Председателем комиссии:

2.6.1. делается запись в Акте контроля соответствия обработки персональных данных о мероприятиях по устранению нарушений и сроках их исполнения;

2.6.2. информация о нарушениях и о мерах для их устранения доводится до сведения руководителя организации.

2.7. В ходе внутренней проверки контролирующие проводят:

— контроль соответствия обработки персональных данных требованиям законодательства, нормативных актов по вопросам обработки персональных данных;

— контроль выполнения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

— проверку параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

— анализ изменения угроз безопасности персональных данных в информационной системе Оператора, возникающих в ходе её эксплуатации;

— контроль наличия или отсутствия фактов несанкционированного доступа к персональным данным;

— контроль соблюдения работниками, допущенными к обработке персональных данных, «Положения об обработке персональных данных», «Инструкции по порядку уничтожения и обезличивания персональных данных», «Инструкции по учёту и хранению съёмных носителей персональных данных», «Положения о порядке доступа в помещения» и других локальных актов, регламентирующих обработку персональных данных Оператора;

— проверку «Журнала учёта съёмных носителей персональных данных»

3. Ответственность

3.1. За организацию проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства отвечает Ответственный либо Председатель комиссии.

3.2. Ответственность за соблюдение Инструкции возлагается на всех работников Оператора, на которых распространяется Инструкция.

Ознакомлены:

Алексеева Д.С.
Андрющенко И.М.
Близнюк Н.А.
Белан В.О.
Будлянская Ю.В.
Ваганова В.Б.
Власенко О.А.
Волошенко А.С.
Гаврищака И.Н.
Галицына Н.Д.
Гендель Т.Г.
Дурасова А.Н.
Ельникова Е.В.
Жогло Т.Б.
Заика А.Н.
Залозний С.А.
Захарина Н.Н.
Иваненко Р.А.
Кадырова Л.В.
Кандаурова Н.Г.
Кашина О.А.
Кисиль О.Ю.
Коваль Н.В.
Коломиец С.В.
Коломиец Г.Г.
Кулинич С.П.
Куцевол О.И.
Лагун В.Н.
Ларина В.А.
Левченко Е.Н.
Матвиенко Т.В.
Мельникова Ю.Ю.
Метченко Г.Н.
Милосердова В.А.
Михайленко Т.В.

Мосиенко Е.В.
Никитина Т.Н.
Оверченко И.А.
Олейник М.Н.
Пасюта Н.В.
Панченко Л.В.
Подпорина Е.Ю.
Подсекина И.И.
Пономарева А.С.
Потурнак Е.Ю.
Пташенко Л.Б.
Ровная Е.В
Ровная Е.В. (л)
Рой Ю.С.
Рыжая В.С.
Савранская Н.П.
Семёнова В.В.
Скворцова Т.И.
Слесаренко Т.Ю.
Стороженко Е.В.
Стрюк О.В.
Терешок О.Г.
Тертица И.Б.
Тололина Н.Г.
Уткина Г.А.
Филобок Е.И.
Фоменко Е.В.
Ханина Н.В.
Цапко Г.А.
Черемскина Л.П.
Чёрная Т.Я.
Шевцова К.А.
Шелуха Ю.В.
Швидченко М.И.
Шупенко Е.А.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

Инструкция
по организации резервирования
и восстановления программного обеспечения,
баз персональных данных информационной системы
персональных данных муниципального автономного
общеобразовательного учреждения средней общеобразовательной
школы № 2 имени Ивана Михайловича Суворова
станицы Павловской

1. Настоящая инструкция разработана с целью обеспечения возможности незамедлительного восстановления персональных данных в информационной системе персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской

2. Резервированию подлежат базы данных и файлы, содержащие персональные данные.

3. Резервирование выполняется штатным средством архивирования системы и данных «ntbackup» и производится на локальный дисковый массив. Процедура резервного копирования производится каждый день.

4. Ответственным за процедуру резервирования и восстановления назначается ответственный за организацию обработки персональных данных.

5. Восстановление файлов производится путем разархивирования файлов базы данных в исходный каталог.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П.

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

– Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав

информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

– Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

– Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

– Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

– Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

– Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

– Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

– Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

– Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

– Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

– Обязан проводить мероприятия по организации антивирусной защиты;

– Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

– Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

– Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

– Установить причины, по которым стал возможным НСД;

– Установить последствия, к которым привел НСД;

– Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

– Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

– Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности

Администратор информационной безопасности имеет право:

– Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

– Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

– Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____Н.Н. Богданова
«31» августа 2020 г.
М.П.

ИНСТРУКЦИЯ
ответственного за эксплуатацию информационных систем персональных данных в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Общие положения

Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской (далее – МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской) назначается Директором.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П.

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

– Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

– Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

– Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по

вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;

– Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;

– Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

4. Права

Ответственный за организацию обработки персональных данных имеет право:

– Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;

Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П.

Инструкция
по антивирусной защите в информационных системах персональных данных муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Настоящая инструкция разработана с целью защиты персональных данных от несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.
2. Пользователи ИСПДн при работе со съемными носителями обязаны перед началом работы осуществить их проверку на предмет наличия компьютерных вирусов.
3. Ответственный за обеспечение безопасности персональных данных настраивает антивирусное средство на автоматическое обновление и ведет за ним контроль.
4. Ответственный за обеспечение безопасности персональных данных проводит периодическое тестирование всех элементов ИСПДн и установленного программного обеспечения на предмет наличия компьютерных вирусов.
5. Использование для обработки и хранения персональных данных неучтенных носителей запрещается.
6. При обнаружении компьютерного вируса пользователи ИСПДн обязаны немедленно поставить в известность ответственного за обеспечение безопасности персональных данных и прекратить какие-либо действия в соответствующей ИСПДн.
7. Ответственный за обеспечение безопасности персональных данных при обнаружении компьютерного вируса принимает меры для «лечения» зараженного файла и удаления вируса и после этого вновь проводит антивирусный контроль.
8. В случае обнаружения на учтенном в Журнале учёта съёмных носителей персональных данных носителе вируса, не поддающегося лечению, ответственный за обеспечение безопасности персональных данных обязан:
— запретить использование носителя;
— поставить в известность ответственного за организацию обработки персональных данных;
— запретить работу в ИСПДн;
— в возможно короткие сроки обновить пакет антивирусных программ.

Ознакомлены:

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____Н.Н. Богданова
«31» августа 2020 г.
М.П.

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Общие положения

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской (далее – МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской), или сотруднику (далее – субъекту персональных данных) МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской или лица, осуществляющие такую обработку по договору с МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, 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 учреждением способов обработки персональных данных;

– типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;

– 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.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала должна быть предусмотрена актом МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

– копирование содержащейся в таких журналах информации не допускается;

– персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

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, зачеркивание, стирание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации 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. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться 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.

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

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

Инструкция
по проведению инструктажа лиц,
допущенных к работе с информационной системой
персональных данных муниципального автономного
общеобразовательного учреждения средней общеобразовательной
школы № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской (далее - ИСПДн).
2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее - новый сотрудник), ответственный за организацию обработки персональных данных:
а) в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами организации в отношении обработки персональных данных, перечисленными в Приложении № 1 к данной инструкции;
б) знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;
в) отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.
3. Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

Ознакомлены:

Приложение 1
к Инструкции по проведению инструктажа лиц,
допущенных к работе с информационными системами
персональных данных

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа

Законодательные акты Российской Федерации о персональных данных:

1) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014).

2) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные в том числе без использования средств автоматизации).

Внутренние локальные акты управления образованием администрации муниципального образования Павловский район

1) Приказ о допуске к обработке персональных данных.
2) Политика в отношении обработки персональных данных.
3) Положение об обработке персональных данных.
4) Положение о порядке доступа в помещения, в которых ведётся обработка персональных данных.
5) Положение об обработке персональных данных без использования средств автоматизации.
6) Инструкция по учёту и хранению съёмных носителей персональных данных.
7) Инструкция по организации резервного копирования и восстановления в ИСПДн.
8) Инструкция по учёту лиц, допущенных к обработке.
9) Инструкция по антивирусной защите.
10) Инструкция по проведению инструктажа лиц, допущенных к работе с ПДн.
11) Инструкция по проведению внутреннего контроля.
12) Инструкция по порядку уничтожения и обезличивания персональных данных.
13) Инструкция пользователя ИСПДн.
14) Инструкция пользователя при возникновении нештатной ситуации.
15) План проведения внутреннего контроля.
16) Приказ об утверждении перечня помещений, в которых ведется обработка.

Приложение 2
к Инструкции по проведению инструктажа лиц,
допущенных к работе с информационными системами
персональных данных

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____Н.Н. Богданова
«31» августа 2020 г.
М.П

ЖУРНАЛ УЧЁТА
прохождения первичного инструктажа работниками,
допущенными к работе с ПДн в ИСПДн

№ п/п	ФИО работника	Дата прохождения инструктажа	Подпись работника	ФИО должностного лица, проводившего инструктаж	Подпись должностного лица
1	2	3	4	5	6

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____Н.Н. Богданова
«31» августа 2020 г.
М.П

ИНСТРУКЦИЯ
по проверке электронного журнала обращений к информационной системе персональных данных в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Задачи проверки.

Под проверкой понимается отслеживание событий, происходивших на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени.

Общими задачами проверки являются:

– Контролирование состояния защищенности системы;

– Выявление причин произошедших изменений;

– Определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;

– Установление времени изменений.

Проверку средств защиты осуществляет администратор информационной безопасности.

2. Журналы записей о событиях.

События, происходящие на АРМ, входящем в состав ИСПДн, регистрируются в журналах.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В состав используемых в ИСПДн средств защиты информации может входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее — программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

– Штатные журналы операционной системы Windows;

– Журналы событий средств защиты информации.

3. Штатные журналы операционной систем.

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

– Журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;

– Системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;

– Журнал безопасности – хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows — в оснастке «Просмотр событий» («Eventviewer»).

4. Журнал событий средств защиты информации.

Журналы средств защиты информации (далее – СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

5. Аудит.

Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.) подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

6. Просмотр событий электронных журналов.

Администратор информационной безопасности в ИСПДн производит проверку электронных журналов.

В случае обнаружения нарушений администратор информационной безопасности докладывает о данном факте ответственному за организацию обработки персональных данных.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

Инструкция пользователя
информационной системы персональных данных
при возникновении нештатных ситуаций в МАОУ СОШ № 2
им.И.М. Суворова ст.Павловской

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных управления образованием администрации муниципального образования Павловский район (далее - ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.
2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работоспособности в случае реализации рассматриваемых угроз.
3. Задачами данной Инструкции являются:
— определение мер защиты от прерывания работоспособности;
— определение действий по восстановлению в случае прерывания работоспособности.
4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
— системы жизнеобеспечения;
— системы обеспечения отказоустойчивости;
— системы резервного копирования и хранения данных;
— системы контроля физического доступа.
5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении № 1.
6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:
— Уровень 1. Незначительный инцидент - локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты;
— Уровень 2. Авария - любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;
— Уровень 3. Катастрофа - любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к

уничтожению, блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни пользователей ИСПДн.

7. При возникновении нештатной ситуации любого уровня пользователь обязан оповестить ответственного за организацию обработки персональных данных, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

8. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности оборудования или ИСПДн. В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

9. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

— системы жизнеобеспечения;
— системы обеспечения отказоустойчивости;
— системы резервного копирования и хранения данных;
— системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

— пожарные сигнализации и системы пожаротушения;
— системы вентиляции и кондиционирования;
— системы резервного питания.

Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных ИСПДн.

10. Ответственный за организацию обработки персональных данных:

— ознакомляет всех сотрудников, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;
— обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Пользователи ИСПДн должны получить базовые знания в следующих областях:

— оказание первой медицинской помощи;
— пожаротушение;
— эвакуация людей;
— защита материальных и информационных ресурсов;
— методы оперативной связи со службами спасения и руководителями структурных подразделений;
— выключение оборудования, электричества, водоснабжения,

газоснабжения;
— по окончанию ознакомления сотрудников получает их роспись в Журнале учета прохождения первичного инструктажа.
11. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данных. Директор школы согласует сроки и порядок их обучения.

Ознакомлены:

Приложение 1 к Инструкции пользователя ИСПДн при возникновении нештатной ситуации

Источники угроз безопасности персональных данных

Технологические угрозы:

— Пожар в здании;

— Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);

— Взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);

— Химический выброс в атмосферу.

Внешние угрозы:

— Массовые беспорядки;

— Сбои общественного транспорта;

— Эпидемия;

— Массовое отравление персонала;

— Теракт.

Стихийные бедствия:

— Удар молнии;

— Сильный снегопад;

— Сильные морозы;

— Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;

— Затопление водой в период паводка;

— Наводнение, вызванное проливным дождем;

— Торнадо;

— Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

ИТ-угрозы:

— Сбой системы кондиционирования в серверном помещении;

— Выход из строя файлового сервера ;

— Частичная потеря информации на сервере без потери его работоспособности;

— Выход из строя локальной сети;

— Выход из строя рабочей станции;

— Частичная потеря информации на рабочей станции без потери её работоспособности. Угроза, связанная с человеческим фактором:

— Ошибка персонала, имеющего доступ к элементам ИСПДн;

— Нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками:

— Отключение электроэнергии;

— Сбой в работе интернет-провайдера;

— Физический разрыв внешних каналов связи.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

ИНСТРУКЦИЯ

по работе с инцидентами информационной безопасности в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской

Ответственность за выявление инцидентов ИБ и реагирование на них в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской (далее – МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской) возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед руководителем МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

- даты и времени;
- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
- информации о последствиях;

– информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПД и юридические последствия для МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных руководителем МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

– замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
– установка дополнительного ПО;
– изменение сетевых настроек рабочего места;
– замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

Инструкция
по учёту и хранению съёмных носителей персональных данных в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Общие положения

1.1. Настоящая «Инструкция по учёту и хранению съёмных носителей персональных данных» (далее — Инструкция) определяет порядок работы со съёмными носителями персональных данных в управлении образованием администрации муниципального образования Павловский район (далее — Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомятся под подпись и выполняют её все лица, допущенные к обработке персональных данных «Приказом о допуске к обработке персональных данных».

2. Определения

Съёмный носитель персональных данных — носитель информации, используемый для хранения и передачи персональных данных в электронной форме.

Пользователь — работник Оператора или сотрудник по договору гражданско-правового характера, допущенный к обработке персональных данных «Приказом о допуске к обработке персональных данных».

3. Порядок работы со съёмными носителями

3.1. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, выдаёт съёмные носители пользователям только в случаях производственной необходимости.

3.2. Все съёмные носители персональных данных учитываются и выдаются пользователям под подпись.

3.3. Пользователям, получившим съёмные носители персональных данных под подпись, запрещается передавать их третьим лицам.

3.4. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, изымает съёмные носители персональных данных при увольнении пользователя.

3.5. Все съёмные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

3.6. Допускается хранение съёмных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов) при условиях уничтожения персональных данных в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных, либо если на съёмном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.
3.7. Право на перемещение съёмных носителей информации за пределы территории, на которой осуществляется обработка, имеют только те лица, которым это необходимо для выполнения своих должностных обязанностей.
3.8. Использование неучтённых съёмных носителей для обработки персональных данных фиксируется как несанкционированное, а ответственный за обеспечение безопасности персональных данных инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения расследования инцидента.
3.9. Пользователи, в случаях утраты или кражи съёмных носителей персональных данных, сообщают об этом ответственному за обеспечение безопасности персональных данных.
3.10. Съёмные носители персональных данных, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных. По результатам уничтожения составляется Акт уничтожения персональных данных.

4. Порядок организации учёта съёмных носителей

4.1. На каждом съёмном носителе персональных данных размещается этикетка с уникальным учётным номером.
4.2. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, при выдаче, приёме, уничтожении съёмных носителей персональных данных вносит в Журнал учета съёмных носителей персональных данных (Приложение 1):
— учётный номер, размещённый на этикетке на съёмном носителе персональных данных;
— тип съёмного носителя (USB-накопитель, внешний жёсткий диск, CD/DVD диск);
— серийный или инвентарный номер съёмного носителя;
— место хранения (номер запираемого шкафа или сейфа, номер помещения);
— дату и номер Акта уничтожения персональных данных в случае уничтожения съёмного носителя;
— подпись.
4.3. Пользователи при получении либо сдаче съёмных носителей персональных данных заносят в Журнал учёта съёмных носителей персональных данных свои фамилию, имя, отчество, ставят дату и подпись.

5. Ответственность

5.1. Все работники Оператора, допущенные в установленном порядке к работе с персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с персональными данными.

5.2. Ответственность за доведение требований настоящей Инструкции до работников Оператора несёт ответственный за организацию обработки персональных данных.

5.3. Ответственность за обеспечение мероприятий по реализации требований настоящей Инструкции, в том числе учёт, выдачу, уничтожение съёмных носителей персональных данных несёт ответственный за обеспечение безопасности персональных данных.

Ознакомлены:

Приложение 1
к Инструкции по учёту и хранению съёмных
носителей персональных данных

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П.

ЖУРНАЛ УЧЁТА
съёмных носителей персональных данных в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской

№ п/п	Учётный номер	Тип носителя	Номер (серийный/ инвентарный)	Место хранения	Расписка в получении		Дата и номер акта уничтожения	Подпись ответственного лица	Примечание
					ФИО, дата получения, подпись	ФИО, дата сдачи, подпись			
1	2	3	4	5	6	7	8	9	10

Алексеева Д.С.
Андрющенко И.М.
Близнюк Н.А.
Белан В.О.
Будлянская Ю.В.
Ваганова В.Б.
Власенко О.А.
Волошенко А.С.
Гаврищака И.Н.
Галицына Н.Д.
Гендель Т.Г.
Дурасова А.Н.
Ельникова Е.В.
Жогло Т.Б.
Заика А.Н.
Залозний С.А.
Захарина Н.Н.
Иваненко Р.А.
Кадырова Л.В.
Кандаурова Н.Г.
Кашина О.А.
Кисиль О.Ю.
Коваль Н.В.
Коломиец С.В.
Коломиец Г.Г.
Кулинич С.П.
Куцевол О.И.
Лагун В.Н.
Ларина В.А.
Левченко Е.Н.
Матвиенко Т.В.
Мельникова Ю.Ю.
Метченко Г.Н.
Милосердова В.А.
Михайленко Т.В.

Мосиенко Е.В.
Никитина Т.Н.
Оверченко И.А.
Олейник М.Н.
Пасюта Н.В.
Панченко Л.В.
Подпорина Е.Ю.
Подсекина И.И.
Пономарева А.С.
Потурнак Е.Ю.
Пташенко Л.Б.
Ровная Е.В
Ровная Е.В. (л)
Рой Ю.С.
Рыжая В.С.
Савранская Н.П.
Семёнова В.В.
Скворцова Т.И.
Слесаренко Т.Ю.
Стороженко Е.В.
Стрюк О.В.
Терешок О.Г.
Тертица И.Б.
Тололина Н.Г.
Уткина Г.А.
Филобок Е.И.
Фоменко Е.В.
Ханина Н.В.
Цапко Г.А.
Черемскина Л.П.
Чёрная Т.Я.
Шевцова К.А.
Шелуха Ю.В.
Швидченко М.И.
Шупенко Е.А.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____Н.Н. Богданова
«31» августа 2020 г.
М.П

Инструкция пользователя
информационных систем персональных данных
муниципального автономного общеобразовательного учреждения
средней общеобразовательной школы № 2 имени Ивана Михайловича
Суворова станицы Павловской

1. Пользователем информационных систем персональных данных муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской (далее - Пользователь) является любой работник МАОУ СОШ № 2 им. И.М. Суворова ст. Павловской, осуществляющий обработку персональных данных в информационных системах персональных данных МАОУ СОШ № 2 им. И.М. Суворова ст. Павловской (далее - ИСПДн).

Согласно ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (далее - ПДн).

2. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обеспечении безопасности ПДн, руководящими и нормативными документами, с которыми он был ознакомлен при прохождении первичного инструктажа.

3. Пользователь несет персональную ответственность за свои действия.

4. Пользователь обязан:

— знать и выполнять требования Положения об обработке данных, Политики в отношении обработки данных, других локальных актов оператора в отношении персональных данных;

— знать и выполнять установленные требования по режиму обработки ПДн, учету, хранению и использованию носителей ПДн, обеспечению безопасности ПДн;

— соблюдать требования парольной политики;

— блокировать АРМ в случае отсутствия на рабочем месте;

— оповещать ответственного за обеспечение безопасности ПДн о фактах нарушения информационной безопасности и возникновения нештатных ситуаций;

— при возникновении нештатных и аварийных ситуаций действовать согласно Инструкции пользователя при возникновении нештатных ситуаций

с целью ликвидации их последствий и возможного ущерба.

5. Пользователю запрещается:

— разглашать обрабатываемые ПДн;

— производить несанкционированное копирование ПДн на учтенные носители;

— производить копирование ПДн на неучтенные носители;

— оставлять незаблокированным АРМ при отсутствии на рабочем месте;

— сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИСПДн.

6. За нарушение информационной безопасности Пользователь несет ответственность согласно действующему законодательству Российской Федерации.

Ознакомлены:

Алексеева Д.С.
Андрющенко И.М.
Близнюк Н.А.
Белан В.О.
Будлянская Ю.В.
Ваганова В.Б.
Власенко О.А.
Волошенко А.С.
Гаврищака И.Н.
Галицына Н.Д.
Гендель Т.Г.
Дурасова А.Н.
Ельникова Е.В.
Жогло Т.Б.
Заика А.Н.
Залозний С.А.
Захарина Н.Н.
Иваненко Р.А.
Кадырова Л.В.
Кандаурова Н.Г.
Кашина О.А.
Кисиль О.Ю.
Коваль Н.В.
Коломиец С.В.
Коломиец Г.Г.
Кулинич С.П.
Куцевол О.И.
Лагун В.Н.
Ларина В.А.
Левченко Е.Н.
Матвиенко Т.В.
Мельникова Ю.Ю.
Метченко Г.Н.
Милосердова В.А.
Михайленко Т.В.

Мосиенко Е.В.
Никитина Т.Н.
Оверченко И.А.
Олейник М.Н.
Пасюта Н.В.
Панченко Л.В.
Подпорина Е.Ю.
Подсекина И.И.
Пономарева А.С.
Потурнак Е.Ю.
Пташенко Л.Б.
Ровная Е.В
Ровная Е.В. (л)
Рой Ю.С.
Рыжая В.С.
Савранская Н.П.
Семёнова В.В.
Скворцова Т.И.
Слесаренко Т.Ю.
Стороженко Е.В.
Стрюк О.В.
Терешок О.Г.
Тертица И.Б.
Тололина Н.Г.
Уткина Г.А.
Филобок Е.И.
Фоменко Е.В.
Ханина Н.В.
Цапко Г.А.
Черемскина Л.П.
Чёрная Т.Я.
Шевцова К.А.
Шелуха Ю.В.
Швидченко М.И.
Шупенко Е.А.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П.

Инструкция
по порядку уничтожения и обезличивания персональных данных в ИСПДн муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Общие положения

1.1. Настоящая инструкция определяет порядок уничтожения и обезличивания информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской (далее — Оператор).

1.2. Инструкция разработана в соответствии с ч. 7 ст. 5, ч. 4 ст. 21 и п. 9 ч. 1 ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ», утверждёнными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 и иными нормативными правовыми актами РФ в области защиты персональных данных.

2. Условия и порядок уничтожения информации, содержащей персональные данные

2.1. Оператор уничтожает информацию, содержащую персональные данные:
— по достижении целей обработки или в случае утраты необходимости в достижении этих целей;
— по достижении окончания срока хранения;
— при наступлении иных законных оснований.

2.2. Уничтожение информации, содержащей персональные данные, производится в случае достижения цели обработки в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

2.3. Уничтожение информации, содержащей персональные данные, производится в случае выявления неправомерной обработки в срок, не превышающий десяти дней с момента выявления неправомерной обработки персональных данных.

2.4. Ответственными за уничтожение информации, содержащей персональные данные, назначаются ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в

информационной системе Оператора. Ответственные лица подписывают соответствующий «Акт об уничтожении персональных данных» (Приложение 1).

2.5. К персональным данным, хранимым в электронном виде, относятся файлы, папки, электронные архивы на жестком диске компьютера и съёмных машинных носителях (компакт-дисках CD-R/RW или DVD-R/RW, дискетах 3,5, флеш-носителях).

2.6. Съёмные машинные носители по истечению сроков обработки и хранения на них персональных данных подлежат уничтожению с целью невозможности восстановления и дальнейшего использования. Это достигается путем деформирования, нарушения единой целостности носителя или его сжигания.

2.7. В случае допустимости повторного использования съёмного машинного носителя применяется программное удаление («затирание») содержимого путём его форматирования с последующей записью новой информации на данный носитель.

2.8. Подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске информационной системы персональных данных, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

2.9. Черновики документов, испорченные листы, варианты и неподписанные проекты документов уничтожаются путём их сожжения или измельчения или другим путем, исключающим восстановление текста документов.

3. Условия и порядок обезличивания информации, содержащей персональные данные

3.1. Оператор может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

— замена части данных идентификаторами;

— обобщение, изменение или удаление части данных;

— деление данных на части и обработка в разных информационных системах;

— перемешивание данных;

— другие способы.

3.3. В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.

3.4. Ответственный за организацию обработки персональных данных назначается ответственным за проведение мероприятий по обезличиванию персональных данных.

3.5. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный за организацию обработки персональных данных.

3.6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.7. Обезличенные персональные данные могут обрабатываться с

использованием и без использования средств автоматизации.

3.8. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

3.9. В процессе обработки обезличенных данных, при необходимости, может производиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

3.10. Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

4. Ответственность

4.1. Ответственность за осуществление контроля выполнения требований настоящей инструкции несет ответственный за организацию обработки персональных данных Оператора.

4.2. Ответственность за выполнение настоящей инструкции возлагается на ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных и всех работников Оператора, допущенных к обработке обезличенных персональных данных, в соответствии с действующим законодательством.

Ознакомлены:

Приложение 1
к Инструкции по порядку уничтожения и
обезличивания персональных данных

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П

АКТ
уничтожения персональных данных

Ответственным за организацию обработки персональных данных проведены следующие мероприятия по уничтожению информации, содержащей персональные данные, в информационной системе персональных данных МАОУ СОШ № 2 им.И.М. Суворова ст.Павловской:

1. Определение носителей персональных данных, цели обработки которых достигнуты или необходимость достижения целей обработки утрачена, либо достигнуто окончание срока хранения.

2. Уничтожение указанных в п. 1 носителей в соответствии с Таблицей 1:

№ п/п	Название, дата, рег. № носителя	Тип носителя	Метод гарантированного уничтожения информации

Ответственный за организацию обработки
персональных данных _____

Алексеева Д.С.
Андрющенко И.М.
Близнюк Н.А.
Белан В.О.
Будлянская Ю.В.
Ваганова В.Б.
Власенко О.А.
Волошенко А.С.
Гаврищака И.Н.
Галицына Н.Д.
Гендель Т.Г.
Дурасова А.Н.
Ельникова Е.В.
Жогло Т.Б.
Заика А.Н.
Залозний С.А.
Захарина Н.Н.
Иваненко Р.А.
Кадырова Л.В.
Кандаурова Н.Г.
Кашина О.А.
Кисиль О.Ю.
Коваль Н.В.
Коломиец С.В.
Коломиец Г.Г.
Кулинич С.П.
Куцевол О.И.
Лагун В.Н.
Ларина В.А.
Левченко Е.Н.
Матвиенко Т.В.
Мельникова Ю.Ю.
Метченко Г.Н.
Милосердова В.А.
Михайленко Т.В.

Мосиенко Е.В.
Никитина Т.Н.
Оверченко И.А.
Олейник М.Н.
Пасюта Н.В.
Панченко Л.В.
Подпорина Е.Ю.
Подсекина И.И.
Пономарева А.С.
Потурнак Е.Ю.
Пташенко Л.Б.
Ровная Е.В
Ровная Е.В. (л)
Рой Ю.С.
Рыжая В.С.
Савранская Н.П.
Семёнова В.В.
Скворцова Т.И.
Слесаренко Т.Ю.
Стороженко Е.В.
Стрюк О.В.
Терешок О.Г.
Тертица И.Б.
Тололина Н.Г.
Уткина Г.А.
Филобок Е.И.
Фоменко Е.В.
Ханина Н.В.
Цапко Г.А.
Черемскина Л.П.
Чёрная Т.Я.
Шевцова К.А.
Шелуха Ю.В.
Швидченко М.И.
Шупенко Е.А.

УТВЕРЖДАЮ
И.о. директора МАОУ СОШ № 2
им. И.М. Суворова ст. Павловской
_____ Н.Н. Богданова
«31» августа 2020 г.
М.П.

Инструкция
по порядку уничтожения и обезличивания персональных данных в ИСПДн муниципального автономного общеобразовательного учреждения средней общеобразовательной школы № 2 имени Ивана Михайловича Суворова станицы Павловской

1. Общие положения

1.1. Настоящая инструкция определяет порядок уничтожения и обезличивания информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в муниципальном автономном общеобразовательном учреждении средней общеобразовательной школе № 2 имени Ивана Михайловича Суворова станицы Павловской (далее — Оператор).

1.2. Инструкция разработана в соответствии с ч. 7 ст. 5, ч. 4 ст. 21 и п. 9 ч. 1 ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ», утверждёнными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 и иными нормативными правовыми актами РФ в области защиты персональных данных.

2. Условия и порядок уничтожения информации, содержащей персональные данные

2.1. Оператор уничтожает информацию, содержащую персональные данные:
— по достижении целей обработки или в случае утраты необходимости в достижении этих целей;
— по достижении окончания срока хранения;
— при наступлении иных законных оснований.

2.2. Уничтожение информации, содержащей персональные данные, производится в случае достижения цели обработки в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

2.3. Уничтожение информации, содержащей персональные данные, производится в случае выявления неправомерной обработки в срок, не превышающий десяти дней с момента выявления неправомерной обработки персональных данных.

2.4. Ответственными за уничтожение информации, содержащей персональные данные, назначаются ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в

информационной системе Оператора. Ответственные лица подписывают соответствующий «Акт об уничтожении персональных данных» (Приложение 1).

2.5. К персональным данным, хранимым в электронном виде, относятся файлы, папки, электронные архивы на жестком диске компьютера и съёмных машинных носителях (компакт-дисках CD-R/RW или DVD-R/RW, дискетах 3,5, флеш-носителях).

2.6. Съёмные машинные носители по истечению сроков обработки и хранения на них персональных данных подлежат уничтожению с целью невозможности восстановления и дальнейшего использования. Это достигается путем деформирования, нарушения единой целостности носителя или его сжигания.

2.7. В случае допустимости повторного использования съёмного машинного носителя применяется программное удаление («затирание») содержимого путём его форматирования с последующей записью новой информации на данный носитель.

2.8. Подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске информационной системы персональных данных, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

2.9. Черновики документов, испорченные листы, варианты и неподписанные проекты документов уничтожаются путём их сожжения или измельчения или другим путем, исключающим восстановление текста документов.

3. Условия и порядок обезличивания информации, содержащей персональные данные

3.1. Оператор может обезличивать персональные данные в статистических или иных исследовательских целях, по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

— замена части данных идентификаторами;
— обобщение, изменение или удаление части данных;
— деление данных на части и обработка в разных информационных системах;
— перемешивание данных;
— другие способы.

3.3. В случае достижения целей обработки персональных данных или в случае утраты необходимости в достижении этих целей способом обезличивания является уменьшение перечня обрабатываемых данных.

3.4. Ответственный за организацию обработки персональных данных назначается ответственным за проведение мероприятий по обезличиванию персональных данных.

3.5. Решение о необходимости обезличивания персональных данных и способе обезличивания принимает ответственный за организацию обработки персональных данных.

3.6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

3.7. Обезличенные персональные данные могут обрабатываться с

использованием и без использования средств автоматизации.

3.8. При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

3.9. В процессе обработки обезличенных данных, при необходимости, может производиться деобезличивание. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

3.10. Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

4. Ответственность

4.1. Ответственность за осуществление контроля выполнения требований настоящей инструкции несет ответственный за организацию обработки персональных данных Оператора.

4.2. Ответственность за выполнение настоящей инструкции возлагается на ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных и всех работников Оператора, допущенных к обработке обезличенных персональных данных, в соответствии с действующим законодательством.

Ознакомлены:

Алексеева Д.С.
Андрющенко И.М.
Близнюк Н.А.
Белан В.О.
Будлянская Ю.В.
Ваганова В.Б.
Власенко О.А.
Волошенко А.С.
Гаврищака И.Н.
Галицына Н.Д.
Гендель Т.Г.
Дурасова А.Н.
Ельникова Е.В.
Жогло Т.Б.
Заика А.Н.
Залозний С.А.
Захарина Н.Н.
Иваненко Р.А.
Кадырова Л.В.
Кандаурова Н.Г.
Кашина О.А.
Кисиль О.Ю.
Коваль Н.В.
Коломиец С.В.
Коломиец Г.Г.
Кулинич С.П.
Куцевол О.И.
Лагун В.Н.
Ларина В.А.
Левченко Е.Н.
Матвиенко Т.В.
Мельникова Ю.Ю.
Метченко Г.Н.
Милосердова В.А.
Михайленко Т.В.

Мосиенко Е.В.
Никитина Т.Н.
Оверченко И.А.
Олейник М.Н.
Пасюта Н.В.
Панченко Л.В.
Подпорина Е.Ю.
Подсекина И.И.
Пономарева А.С.
Потурнак Е.Ю.
Пташенко Л.Б.
Ровная Е.В
Ровная Е.В. (л)
Рой Ю.С.
Рыжая В.С.
Савранская Н.П.
Семёнова В.В.
Скворцова Т.И.
Слесаренко Т.Ю.
Стороженко Е.В.
Стрюк О.В.
Терешок О.Г.
Тертица И.Б.
Тололина Н.Г.
Уткина Г.А.
Филобок Е.И.
Фоменко Е.В.
Ханина Н.В.
Цапко Г.А.
Черемскина Л.П.
Чёрная Т.Я.
Шевцова К.А.
Шелуха Ю.В.
Швидченко М.И.
Шупенко Е.А.