УТВЕРЖДАЮ
Директор техникума
_____ А.Ф. Саланов
«19» мая 2016 г.

ЛОКАЛЬНЫЙ АКТ
(ПРИЛОЖЕНИЕ К УСТАВУ
ОГБПОУ БОЛЬШЕНАГАТКИНСКИЙ ТТиС)

«ПЕРЕЧЕНЬ ЛОКАЛЬНЫХ АКТОВ,
РЕГЛАМЕНТИРУЮЩИХ ДЕЯТЕЛЬНОСТЬ ТЕХНИКУМА»

1.12 Положение
О порядке обработки и защите персональных данных

Принят общим собранием
Трудового коллектива техникума
Протокол №4 от 18.05.2016г.
Председатель собрания
_____ Горлова Е.А.

I. Общие положения

1. Настоящее Положение об обработке и защите персональных данных в ОГБПОУ Большенагаткинский ТТиС (далее - Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников, студентов, абитуриентов и других физических лиц (далее - физические лица, субъекты персональных данных) в ОГБПОУ Большенагаткинский ТТиС (далее - Техникум) в соответствии с законодательством Российской Федерации.

2. Настоящее Положение разработано на основании:

- Конституции Российской Федерации;
- Трудового кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
- Федерального закона от 23.12.2010 №359-ФЗ «О внесении изменений в статью 25 Федерального закона «О персональных данных»;
- Федерального закона от 29.12.2012г. №273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращения граждан Российской Федерации».
- Устава ОГБПОУ Большенагаткинский ТТиС;
- другими определяющими случаи и особенности обработки персональных данных нормативно-правовыми актами.

3. Настоящее Положение регулирует отношения, связанные с обработкой персональных данных, включающие в себя производимые Техникумом действия по получению, хранению, комбинированию, передаче персональных данных физических лиц или иному их использованию, с целью защиты персональных данных субъектов от несанкционированного доступа, а также неправомерного их использования и утраты.

4. Основные понятия, используемые в настоящем Положении:

- персональные данные физического лица - информация, необходимая Техникуму в связи с трудовыми, гражданско-правовыми и иными отношениями и касающаяся конкретного физического лица: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, позволяющая идентифицировать его личность;

- 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 физического лица;

- 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;

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;

- конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

- персональные данные - любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

5. Все персональные сведения о физическом лице Техникум может получить только от него самого. В случаях, когда Техникум может получить необходимые персональные данные физического лица только у третьего лица, Техникум должен уведомить субъекта персональных данных об этом и получить от него письменное согласие.

Техникум обязан сообщить субъекту персональных данных о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

6. Персональные данные физического лица являются конфиденциальной информацией и не могут быть использованы Техникумом, или любым иным лицом в личных целях. Режим конфиденциальности персональных данных

снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

7. Сотрудники Техникума, в обязанность которых входит обработка персональных данных физических лиц, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

8. Сотрудники Техникума, в соответствии со своими полномочиями владеющие информацией о физических лицах, получающие и использующие её, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

9. Настоящее Положение утверждается и вводится в действие приказом директора Техникума и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным субъектов персональных данных.

II. Понятие и состав персональных данных

10. При определении объема и содержания персональных данных субъекта персональных данных Техникум руководствуется Конституцией РФ, Трудовым кодексом РФ. Законом «Об образовании», иными федеральными законами и настоящим Положением.

11. К персональным данным работника, получаемым Техникумом и подлежащим хранению в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах работников:

- паспортные данные работника;
- ИНН;
- копия страхового свидетельства государственного пенсионного страхования;
- копия документа воинского учёта (для военнообязанных и лиц, подлежащих призыву на военную службу);
- копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- анкетные и биографические данные, заполненные работником при поступлении на работу или в процессе работы (в том числе адрес места жительства, телефон, сведения о семейном положении работника, место работы или учебы членов семьи и родственников, 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.);
- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);
- трудовой договор;
- копии приказов о приёме, переводах, увольнении, премировании, поощрениях и взысканиях;
- личная карточка по форме Т-2;
- заявления, объяснительные и служебные записки работника;
- документы о прохождении работником аттестации, повышения квалификации;
- иные документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с

работником (включая приговоры суда о запрете занимаемой педагогической деятельностью или занимать руководящие должности)

12. К персональным данным студентов, слушателей и абитуриентов (далее - обучающееся), получаемым Техникумом и подлежащим хранению в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в личных делах:

- документы, удостоверяющие личность обучающегося (свидетельство о -гудении или паспорт):
- документы о месте проживания;
- документы о составе семьи;
- паспортные данные родителей (законных представителей) обучающегося;
- документы о получении образования, необходимого для поступления в Техникум (аттестат, диплом, академическая справка, справка с предыдущего

. та учебы и т.п.);

- анкетные и биографические данные, заполненные обучающимся при поступлении в Техникум или в процессе обучения (в том числе адрес места жительства, телефон, сведения о семейном положении, место работы или учебы членов семьи и родственников, место работы или учебы членов семьи и родственников, перемене фамилии, наличии детей и иждивенцев);
- полис медицинского страхования;
- 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.);

- иные документы, содержащие персональные данные (в том числе сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством РФ).

13. К персональным данным иных физических лиц, получаемым Техникумом и подлежащим хранению в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения:

- документы, удостоверяющие личность (свидетельство о рождении или паспорт);
- документы о месте проживания;
- документы о составе семьи;
- иные документы, содержащие персональные данные.

Ш. Основные условия проведения обработки персональных данных

14. Техникум определяет объем, содержание обрабатываемых персональных данных работников ,обучающихся и иных физических лиц, руководствуясь Конституцией Российской Федерации. Трудовым кодексом Российской Федерации, Законом РФ от 10.07.1992 № 3266-1 «Об образовании» и иными федеральными законами.

15. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и - движении по службе, а также обеспечения личной безопасности работников, сохранности имущества, контроля количества и качества выполняемой работы.

Обработка персональных данных обучающегося может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов; содействия обучающимся в обучении, трудоустройстве; обеспечения их личной безопасности; контроля качества обучения и обеспечения сохранности имущества.

Обработка персональных данных иных физических лиц может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов; обеспечения их личной безопасности; контроля обеспечения сохранности имущества.

16. Все персональные данные работника предоставляются работником, за исключением случаев, предусмотренных федеральным законом. Если персональные данные работника, возможно, получить только у третьей стороны, то Техникум обязан заранее уведомить об этом работника и получить его письменное согласие. Техникум должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

17. Все персональные данные несовершеннолетнего обучающегося в возрасте до 14 лет предоставляются его родителями (законными представителями). Если персональные данные обучающегося возможно получить только у третьей стороны, то родители (законные представители) обучающихся должны быть уведомлены об этом заранее. От них должно быть е но письменное согласие на получение персональных данных от третьей стороны. Родители (законные представители) обучающегося должны быть проинформированы о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

Персональные данные несовершеннолетнего обучающегося в возрасте старше 14 лет предоставляются самим обучающимся с письменного согласия своих и иных представителей - родителей, усыновителей или попечителя. Если персональные данные обучающегося возможно получить только у третьей стороны, то обучающийся, должен быть уведомлен об этом заранее. От него и его родителей (законных представителей) должно быть получено письменное согласие на получение персональных данных от третьей стороны. Обучающийся его родители (законные представители) должны быть проинформированы о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

Приложения №1 Согласие Законного представителя (родителей) на обработку персональных данных несовершеннолетнего.

Приложение № 2 Согласие
Законного представителя (опекуна, попечителя, приемного родителя) на обработку персональных данных детей - сирот (детей, оставшихся без попечения родителей).

Приложение № 3 Заявление о согласии на обработку персональных данных.

18. Техникум не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его политических, религиозных и иных убеждениях и частной жизни без письменного согласия субъекта персональных данных.

Техникум не имеет права получать и обрабатывать персональные данные

субъекта персональных данных о его членстве в общественных объединениях профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

19. Техникум вправе осуществлять сбор, передачу, уничтожение, хранение, использование информации о политических, религиозных, других убеждениях и жизни, а также информации, нарушающей тайну переписки, телефонных переговоров почтовых, телеграфных и иных сообщений:

- работника, иных физических лиц только с его письменного согласия или на основании судебного решения.

- обучающегося только с его письменного согласия (согласия родителей законных представителей) малолетнего несовершеннолетнего обучающегося) или на основании судебного решения.

20. Техникум не вправе предоставлять персональные данные субъекта персональных данных в коммерческих целях, без письменного согласия субъекта .

IV. Хранение, использование и передача персональных данных

21. Персональные данные субъекта персональных данных хранятся на бумажных и электронных носителях, в специально предназначенных для этого помещениях в специальном шкафу, обеспечивающем защиту от несанкционированного доступа.

Персональные данные субъекта персональных данных могут также храниться в электронном виде на локальной компьютерной сети. Доступ к базам данных, содержащим информацию о персональных данных субъекта персональных данных, обеспечивается системой паролей. Пароли устанавливаются руководителем службы ИКТ и сообщаются индивидуально

сотрудникам, имеющим доступ к персональным данным субъекта персональных данных.

Приложение № 4 Должностные инструкции системного администратора, инструкция по проведению мониторинга информационной безопасности и антивирусного контроля, инструкция по организации парольной защиты).

22. В процессе хранения персональных данных субъектов персональных данных должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;

- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

По истечении срока хранения персональные данные подлежат уничтожению.

23. Нижеперечисленные должностные лица для исполнения возложенных на них должностных обязанностей имеют доступ к персональным данным субъекта персональных данных в Техникуме:

- директор техникума;
- заместители директора;
- главный бухгалтер;
- заведующие отделений (к персональным данным студентов и слушателей соответствующих отделений и специальностей);
- инспектор по кадрам (к персональным данным работников);
- секретарь учебной части (к персональным данным студентов, слушателей и обучающихся);
- классные руководители групп (только к персональным данным студентов своей группы);
- бухгалтер по начислению заработной платы, бухгалтер материальной группы;
- кассир;
- зав. общежитием (к персональным данным проживающих в общежитии);

- руководители подразделений (только к персональным данным своих подчинённых);
- заведующая канцелярией; - специалисты, выполняющие обязанности системного администратора, обслуживающие компьютерное оборудование и лицензионное обеспечение;
- специалисты, выполняющие обязанности системного администратора, обслуживающие компьютерное оборудование и программное обеспечение;
- иные работники, определяемые приказами и распоряжениями директора Техникума в пределах своей компетенции или уполномоченные действующим законодательством.

Приложение № 5. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники.

№ П П	Ф.И.О. работника	Должность	Дата приема на работу	Адрес, телефон	Примечание

№ П П	Ф.И.О. работника	Должность	Дата приема на работу	Адрес, телефон	Примечание

24. Лица, имеющие доступ к персональным данным, обязаны использовать персональные данные субъектов персональных данных лишь в целях, для которых они были предоставлены.

25. Ответственным за организацию и осуществление хранения персональных данных субъектов персональных данных являются:

- инспектор по кадрам техникума - за организацию и осуществление хранения персональных данных работников;
- секретарь учебной части - за организацию и осуществление хранения персональных данных студентов, слушателей и обучающихся;

- главный бухгалтер - за организацию и осуществление хранения персональных данных работников, обучающихся и иных физических лиц, обрабатываемых бухгалтерской службой;

- специалисты, выполняющие работы системного администратора, обслуживающие компьютерное оборудование и программное обеспечение - за организацию и осуществление хранения персональных данных субъектов персональных данных в электронном виде на локальной компьютерной сети.

26. Персональные данные работника отражаются в личной карточке работника (форма Т-2), которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в специально оборудованных несгораемых шкафах в алфавитном порядке.

27. Персональные данные студентов отражаются в его личном деле, которое заполняется после издания приказа о его зачисления в Техникум. Личные дела обучающихся в алфавитном порядке формируются в папках групп, которые хранятся в специально оборудованных несгораемых шкафах.

28. Должностное лицо, получающее доступ к персональным данным, должно обеспечивать конфиденциальность таких данных, за исключением случаев, когда обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

29. Работа с персональными данными организовывается в строгом соответствии с требованиями к обработке и хранению информации ограниченного доступа.

30. При передаче персональных данных работников и обучающихся Техникума, а также иных физических лиц другим юридическим и физическим лицам Техникум должен соблюдать следующие требования:

30.1. Персональные данные субъекта персональных данных не могут быть сообщены третьей стороне без письменного согласия субъектов персональных данных, родителей (законных представителей) несовершеннолетнего (малолетнего) обучающегося, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника (обучающегося), а также в случаях, установленных федеральным законом.

30.2. Лица, получающие персональные данные субъекта персональных данных должны предупреждаться о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Техникум должен требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

31. Государственные и негосударственные функциональные структуры (налоговые инспекции, правоохранительные органы, органы статистики, страховые агентства, военкоматы, органы социального страхования, пенсионные фонды, подразделения муниципальных органов управления и др.) а также контрольно-надзорные органы имеют доступ к информации только в сфере своей компетенции.

32. Передача персональных данных субъекта персональных данных его представителям может быть осуществлена в установленном действующим законодательством порядке только в том объеме, который необходим для выполнения указанными представителями их функций.

V. Обязанности Техникума по хранению и защите персональных данных

33. Техникум обязан:

33.1. За свой счет обеспечить защиту персональных данных субъекта персональных данных от неправомерного их использования или утраты, в порядке, установленном законодательством РФ.

33.2. Ознакомить субъекта персональных данных и его представителей с настоящим Положением и их правами в области защиты персональных данных.

33.3. Осуществлять передачу персональных данных субъекта персональных данных только в соответствии с настоящим Положением и законодательством РФ.

33.4. Предоставлять персональные данные субъекта персональных данных только уполномоченным лицам, и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим Положением и законодательством РФ.

33.5. Обеспечить субъекту персональных данных свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством.

33.6. По требованию субъекта персональных данных предоставить ему полную информацию о его персональных данных и обработке этих данных.

34. Лица, имеющие доступ к персональным данным субъекта, обязаны соблюдать режим конфиденциальности. В связи с режимом конфиденциальности информации персонального характера должны предусматриваться соответствующие меры безопасности для защиты данных от случайного или несанкционированного уничтожения, от случайной утраты, от несанкционированного доступа к ним, изменения или распространения.

Приложение № 7 Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

VI. Права субъектов персональных данных на обеспечение защиты их персональных данных

35. В целях обеспечения защиты персональных данных, хранящихся у Техникума, субъекты персональных данных, в том числе, (родители (законные представители) малолетнего несовершеннолетнего обучающегося), имеют право:

35.1. Получать полную информацию о своих персональных данных и их обработке.

35.2. Свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении субъекта персональных данных (для малолетнего несовершеннолетнего - его родителей, законных представителей) - к соответствующему должностному лицу, ответственному за организацию и осуществление хранения персональных данных субъектов или к директору Техникума.

Приложение №8. Журнал обращений по ознакомлению с персональными данными.

№ п/п	Ф.И.О. субъекта персональных данных	Дата обращения	Запрашиваемый документ (данные)	Отметка о выполнении	Подпись заявителя	Примечание

35.3. Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований действующего законодательства. Указанное требование должно быть оформлено письменным заявлением субъекта на имя директора Техникума.

При отказе директора Техникума исключить или исправить персональные данные субъект персональных данных (родитель, законный представитель несовершеннолетнего обучающегося) имеет право заявить в письменном виде директору Техникума о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект персональных данных (родитель, законный представитель несовершеннолетнего обучающегося) имеет право дополнить заявлением, выражающим его собственную точку зрения.

35.4. Требовать об извещении Техникумом всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных обо всех произведенных в них исключениях, исправлениях или дополнениях.

35.5. Обжаловать в суде любые неправомерные действия или бездействия Техникума при обработке и защите его персональных данных.

VII. Обязанности субъекта персональных данных по обеспечению достоверности его персональных данных

36. В целях обеспечения достоверности персональных данных работники обязаны:

36.1. При приеме на работу в Техникум представлять уполномоченным работникам Техникума достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

36.2. В случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании сообщать, об этом в течение 5 рабочих дней с даты их изменений.

36.3. В случае изменения персональных данных работника о состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом незамедлительно в день их изменения.

37. В целях обеспечения достоверности персональных данных обучающиеся (родители, законные представители несовершеннолетних обучающихся) обязаны:

37.1. При поступлении в Техникум представлять уполномоченным работникам Техникума достоверные сведения о себе (своих несовершеннолетних детях).

37.2. В случае изменения сведений, составляющих персональные данные несовершеннолетнего обучающегося старше 14 лет, он обязан в течение 10 дней сообщить об этом уполномоченному работнику Техникума.

37.3. В случае изменения сведений, составляющих персональные данные обучающегося, родители (законные представители) несовершеннолетнего обучающегося в возрасте до 14 лет обязаны в течение месяца сообщить об этом уполномоченному работнику Техникума.

VIII. Ответственность за нарушение норм, регулирующих обработку персональных данных и настоящего Положения

38. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к:

дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами;

- к гражданско-правовой ответственности по основаниям и в порядке, пгед\ смотренных гражданским законодательством;

- административной ответственности (в соответствии с нормами КоАП РФ);

- уголовной ответственности (в соответствии с нормами УК РФ).

39. За нарушение порядка обработки (сбора, хранения, использования, распространения и защиты) персональных данных должностное лицо несёт административную ответственность в соответствии с действующим законодательством.

40. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несёт материальную ответственность в соответствии с действующим трудовым законодательством.

41. Работник, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, несет дисциплинарную ответственность, вплоть до увольнения.

42. Техникум освобождается от ответственности в случае непредставления или несвоевременного представления субъектом персональных данных достоверных сведений о себе или их изменениях.

43. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

44. Техникум вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);

- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для

исполнения указанного договора и заключения договоров с субъектом персональных данных;

- являющихся общедоступными персональными данными;

- включающих в себя только фамилии, имена и отчества субъектов персональных данных;

- необходимых в целях однократного пропуска субъекта персональных данных на территорию Техникума или в иных аналогичных целях;

- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка (включая базы данных, формируемые в связи с ЕГЭ);

- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Во всех остальных случаях оператор (директор Техникума и (или) уполномоченные им лица) обязан направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

Приложение № 1
к разделу III п. 17 Локального акта № 1.12
«Положение об обработке и защите персональных данных» от 18.05.2016 г.

СОГЛАСИЕ ЗАКОННОГО ПРЕДСТАВИТЕЛЯ (родителей) НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНЕГО

Я,

_____
(Ф.И.О)
Проживающий по адресу:
_____
Паспорт № , выданный (кем
_____
и когда)
_____

как законный представитель на основании
_____ (документ, подтверждающий,
что субъект является законным представителем несовершеннолетнего ребенка) настоящим даю свое согласие на обработку в ОГБПОУ Большенагаткинский ТТиС персональных данных моего несовершеннолетнего ребенка

_____ , к которым относятся:

- документы, удостоверяющие личность (свидетельство о рождении или паспорт);
- документы о месте проживания;
- документы о составе семьи;
- паспортные данные родителей;
- документы о получении образования, необходимого для поступления в Техникум (аттестат, диплом, академическая справка, справка с предыдущего места учебы и т.п.);
-анкетные и биографические данные, заполненные при поступлении в Техникум или в процессе обучения (в том числе адрес места жительства, телефон, сведения о семейном положении, место работы или учебы членов семьи и родственников, место работы или учебы членов семьи и родственников, перемене фамилии, наличии детей и иждивенцев);
-полис медицинского страхования;
-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.);

- иные документы, содержащие персональные данные (в том числе сведения, необходимые для предоставления гарантий и компенсации, установленных действующим законодательством)

Я даю согласие на использование персональных данных моего несовершеннолетнего ребенка в целях:

-обеспечения учебного процесса несовершеннолетнего ребенка;

- медицинского обслуживания;

-ведения статистики.

Настоящее согласие предоставляется на осуществление любых действий в отношении персональных данных моего несовершеннолетнего ребенка, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение • обновление, изменение), использование, распространение (в том числе передачу третьим лицам - Департаменту профессионального образования и охраны прав несовершеннолетних Ульяновской области, районным медицинским учреждениям, военкомату, отделениям милиции и т.д.), обезличивание, блокирование, трансграничную передачу персональных данных, а также -предоставление любых иных действий с моими персональными данными, предусмотренных действующим законодательством РФ.

ОГБПОУ Большенагаткинский ТТиС гарантирует, что обработка персональных данных осуществляется в соответствии с действующим законодательством РФ.

Я проинформирован, что ОГБПОУ Большенагаткинский ТТиС будет обрабатывать персональные данные как неавтоматизированным, так и автоматизированным способом обработки. Данное согласие действует до достижения целей обработки персональных данных моего несовершеннолетнего ребенка в ОГБПОУ Большенагаткинский ТТиС. Согласие может быть отозвано по моему

письменному заявлению. Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в интересах моего несовершеннолетнего ребенка.

Дата:_____ Подпись

_____/_____

Приложение № 2 к разделу III п. 17
Локального акта № 1.12«Положение
об обработке и защите персональных
данных» от 18.05.2016 г.

СОГЛАСИЕ
ЗАКОННОГО ПРЕДСТАВИТЕЛЯ (ОПЕКУНА, ПОПЕЧИТЕЛЯ, ПРИЕМНОГО РОДИТЕЛЯ) НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЕТЕЙ - СИРОТ (ДЕТЕЙ, ОСТАВШИХСЯ БЕЗ ПОПЕЧЕНИЯ РОДИТЕЛЕЙ)

Я_____

Ф.И.О)
Проживающий по адресу:

Паспорт № , выданный (кем и когда)

как законный представитель на основании

(документ, подтверждающий, что субъект является законным представителем ребенка - сироты (ребенка, оставшегося без попечения жителей)) настоящим даю свое согласие на обработку в ОГБПОУ Большенагаткинский ТТиС персональных данных ребенка - сироты (ребенка, оставшегося без попечения родителей) _____ _____ , к которым относятся:

- данные паспорта;
- данные свидетельства о рождении;
- документы о получении образования, необходимого для поступления в Техникум (аттестат, диплом, академическая справка, справка с предыдущего места учебы и т.п.);
- сведения о родителях или лицах их заменяющих (свидетельство о смерти родителей, приговор или решение суда, справка о болезни или розыске родителей, и другие документы, подтверждающие отсутствие родителей или невозможности воспитать своих детей);
- сведения о наличии и месте нахождения (жительства) близких родственников;
- опись имущества (ребенка - сироты) оставшегося после смерти родителей,
- сведения о лицах, отвечающих за их неприкосновенность;
- документы о закреплении жилой площади, ее сохранности;
- справка государственного учреждения Управления пенсионного фонда РФ и пенсионная книжка для получающих пенсию;
- страховое свидетельство государственного пенсионного страхования;
- копия решения суда о взыскании алиментов или копия судебного приказа;
-сберегательная книжка;

- медицинский страховой полис;
- свидетельство о присвоении ИНН;
- данные медицинской карты;
- адрес проживания;
- анкетные и биографические данные, заполненные при поступлении в Техникум или в процессе обучения;
- иные документы, содержащие персональные данные (в том числе сведения, необходимые для предоставления гарантий и компенсаций, установленных действующим законодательством РФ).

Я даю согласие на использование персональных данных ребенка - сироты :(ребёнка оставшегося без попечения родителей) в целях:
-обеспечения учебного процесса ребенка - сироты и ребенка, оставшегося без попечения родителей;
- медицинского обслуживания;
- ведения статистики.

Настоящее согласие предоставляется на осуществление любых действий в отношении персональных данных ребенка - сироты (ребенка, оставшегося без попечения родителей), которые необходимы или желаемы для достижения законных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, -распространение (в том числе передачу третьим лицам - Департаменту профессионального образования и охраны прав несовершеннолетних Ульяновской области, районным медицинским учреждениям, военкомату, отделениям милиции и т.д.), обезличивание, блокирование, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными, предусмотренных действующим законодательством.

ОГБПОУ Большенагаткинский ТТиС гарантирует, что обработка персональных данных осуществляется в соответствии с действующим законодательством РФ.

Я проинформирован, что ОГБПОУ Большенагаткинский ТТиС будет обрабатывать персональные данные как неавтоматизированным, так и автоматизированным способом обработки.

Данное согласие действует до достижения целей обработки персональных данных ребенка - сироты (ребенка, оставшегося без попечения родителей) в ОГБПОУ Большенагаткинский ТТиС

Согласие может быть отозвано по моему письменному заявлению. Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в интересах ребенка -сироты (ребенка, оставшегося без попечения родителей).

Дата: _____ Подпись

_____/ _____/

Представитель (начальник) отдела опеки и
попечительства МО «Цильнинский район»

Приложение № 3
к разделу III п. 17 Локального акта№ 1.12
«Положение об обработке и защите персональных данных» от 18.05.2016 г

Директору ОГБПОУ
Большенагаткинский ТТиС
А.Ф. Саланову

_____
(Ф.И.О. заявителя)
_____

_____

_____
(должность работника)
_____

ЗАЯВЛЕНИЕ о согласии на обработку персональных данных

Не возражаю против получения Вами сведений обо мне, содержащих данные паспорта; ИНН; страхового свидетельства государственного пенсионного страхования; документа воинского учёта (при наличии); документа об образовании; квалификации или наличии специальных знаний; анкетные и биографические данные, заполненные при поступлении на работу или в процессе работы (в том числе адрес места жительства, телефон, сведения о семейном положении работника, место работы или учебы членов семьи и родственников, перемене фамилии, наличии детей и иждивенцев); документов о возрасте малолетних детей и месте их обучения; документов о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний); документов о состоянии здоровья (сведения об инвалидности, о беременности и т.п.); иных документов, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые при прохождении обязательных предварительных и периодических медицинских осмотров); трудового договора; приказов о приёме, переводах, увольнении, премировании, поощрениях и взысканиях; личной карточки по форме Т-2; заявлений, объяснительных и служебных записок; документов о прохождении аттестации, повышения квалификации; иных документов, содержащих сведения, нахождение которых в личном деле необходимо для документального оформления трудовых правоотношений (включая приговоры суда о запрете заниматься педагогической деятельностью или занимать руководящие должности) с целью обработки персональных данных, включающих в себя производимые Техникумом действия

по получению, хранению, комбинированию, передаче персональных данных физических лиц или иному их использованию, для защиты персональных данных субъектов от несанкционированного доступа, а также неправомерного их использования и утраты в устной, документальной, электронной формах на период работы в Техникуме.

Настоящее заявление может быть отозвано мной в письменной форме.

Дата Подпись

/ /

Приложение № 4
к разделу IV п.21 Локального акта № 1.12
«Положение об обработке и защите персональных данных» от 18.05.2016 г

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ СИСТЕМНОГО АДМИНИСТРАТОРА

I. Общие положения

1. Системный администратор относится к категории специалистов.

2. На должность системного администратора назначается лицо, имеющее профильное профессиональное образование, опыт технического обслуживания и ремонта персональных компьютеров и оргтехники, знающее основы локальных сетей (стек протоколов TCP/IP, сетевое оборудование, принципы построения локальных вычислительных сетей).

3. Системный администратор должен знать:

3.1.Технические характеристики, назначение, режимы работы, конструктивные особенности, правила технической эксплуатации оборудования локальных вычислительных сетей, оргтехники, серверов и персональных компьютеров.

3.2. Аппаратное и программное обеспечение локальных вычислительных сетей.

3.3. Принципы ремонта персональных компьютеров и оргтехники.

3.4. Языки и методы программирования.

3.5. Основы информационной безопасности, способы защиты информации от несанкционированного доступа, повреждения или умышленного искажения.

3.6. Порядок оформления технической документации.

3.7. Правила внутреннего трудового распорядка.

3.8. Основы трудового законодательства.

3.9. Правила и нормы охраны труда, техники безопасности и противопожарной защиты.

4. Назначение на должность системного администратора и освобождение от должности производится приказом директора по представлению руководителя отдела IT.

5. Системный администратор подчиняется непосредственно руководителю отдела IT.

II. Должностные обязанности системного администратора

Системный администратор:

1. Устанавливает на серверы и рабочие станции операционные системы и необходимое для работы программное обеспечение.

2.Осуществляет конфигурацию программного обеспечения на серверах и рабочих станциях.

3.Поддерживает в работоспособном состоянии программное обеспечение серверов и рабочих станций.

4.Регистрирует пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.

5.Осуществляет техническую и программную поддержку пользователей, консультирует пользователей по вопросам работы локальной сети и программ, составляет инструкции по работе с программным обеспечением и доводит их до сведения пользователей.

6.Устанавливает права доступа и контролирует использование сетевых ресурсов.

7.Обеспечивает своевременное копирование, архивирование и резервирование данных.

8.Принимает меры по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.

9.Выявляет ошибки пользователей и программного обеспечения и принимает меры по их исправлению.

10.Проводит мониторинг сети, разрабатывает предложения по развитию инфраструктуры сети.

11.Обеспечивает сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.

12.0существляет антивирусную защиту локальной вычислительной сети, серверов и рабочих станций.

13.Готовит предложения по модернизации и приобретению сетевого оборудования.

14.Осуществляет контроль за монтажом оборудования локальной сети специалистами сторонних организаций.

15.Сообщает своему непосредственному руководителю о случаях нарушения правил пользования локальной вычислительной сетью и принятых мерах.

III. Права системного администратора

Системный администратор имеет право:

1 .Устанавливать и изменять правила пользования локальной вычислительной сетью.

2.Знакомиться с документами, определяющими его права и обязанности по занимаемой должности, критерии оценки качества исполнения должностных обязанностей.

3.Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей должностной инструкцией обязанностями.

4.Требовать от руководства обеспечения организационно - технических условий, необходимых для исполнения должностных обязанностей.

IV. Ответственность системного администратора

1. Системный администратор несет ответственность за:

1.1. Нарушение функционирования локальной вычислительной сети, серверов и персональных компьютеров вследствие ненадлежащего исполнения своих должностных обязанностей.

1.2. Несвоевременную регистрацию пользователей локальной вычислительной сети и почтового сервера.

1.3. Несвоевременное уведомление руководства о случаях нарушения правил пользования локальной вычислительной сетью.

2. Системный администратор привлекается к ответственности:

2.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией - в пределах, установленных действующим трудовым законодательством Российской Федерации.

2.2. За правонарушения, совершенные в процессе своей деятельности - в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

2.3. За причинение материального ущерба компании - в пределах, установленных действующим законодательством Российской Федерации.

ИНСТРУКЦИЯ

по проведению мониторинга информационной безопасности и антивирусного контроля

1 Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля (далее - Инструкция) регламентирует порядок планирования и проведения мероприятий, направленных на обеспечение безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации, необходимой в работе образовательного учреждения (далее - ОУ).

2. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны постоянно контролироваться в рамках работы администраторов соответствующих систем.

3. Мониторинг парольной защиты предусматривает:

- контроль соблюдения сроков действия паролей (не более трех месяцев);
- периодическую (не реже одного раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств ("взломщиков" паролей).

4. Мониторинг целостности программного обеспечения включает:

- проверку контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;
- сверку дубликатов идентификаторов пользователей;
- проверку и восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Мероприятия, направленные на предупреждение и своевременное выявление попыток несанкционированного доступа, в т. ч. выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и определяющих места ее уязвимости, осуществляются с использованием средств операционной системы и специальных программных средств. Они должны сопровождаться фиксацией неудачных попыток входа в систему в системном журнале и протоколированием работы сетевых сервисов.

6. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, осуществляется по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности.

Системный аудит производится ежеквартально и в особых ситуациях. Он включает в себя проведение обзоров безопасности, тестирование системы и контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности, и включают:

- составление отчётов о безопасности пользовательских ресурсов (в т. ч. о наличии повторяющихся пользовательских имен и идентификаторов, неправильных форматах регистрационных записей, пользователях без пароля, неправильной установке домашних каталогов пользователей и уязвимостях пользовательских окружений);

- проверку содержимого файлов конфигурации на соответствие списку для проверки;

- анализ данных об обнаружении изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

- оценку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

9. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в информационную систему с помощью автоматического инструментария или вручную.

10. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Сначала информация об известных уязвимостях извлекается из документации и внешних источников, а затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо выполнить одно из следующих действий:

изменить конфигурацию системы (для ликвидации условий проявления уязвимости);

установить программные коррекции либо другие версии программ, в которых данная уязвимость отсутствует;

отказаться от использования системного сервиса, содержащего данную уязвимость.

11. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным соблюдением следующих условий:

документирование изменений в соответствующем журнале;

уведомление работника, которого касается изменение;

анализ претензий, в случае если это изменение причинило кому-нибудь вред;

разработка планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

12. Для защиты от вредоносных программ и вирусов необходимо использовать только лицензионные или сертифицированные свободно распространяемые антивирусные средства.

13. Для защиты серверов и рабочих станций используются:

резидентные антивирусные мониторы, контролирующие подозрительные действия программ; утилиты для обнаружения и анализа новых вирусов.

14. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

15. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

16. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. После установки (изменения) программного обеспечения рабочей станции необходимо провести антивирусную проверку.

17. Запуск антивирусных программ осуществляется автоматически по заданию, созданному с использованием планировщика задач, входящего в поставку операционной системы либо поставляемого вместе с антивирусными программами.

18. Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется проводить полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

19. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации проводится антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

20.Устанавливаемое на и серверы программное обеспечение предварительно проверяется администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

21. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее: осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер; проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

22. На серверах электронной почты следует применять антивирусное программное обеспечение, позволяющее осуществлять проверку всех входящих сообщений. В случае если проверка входящих сообщений на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения блокируется. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

23. Антивирусные базы на всех рабочих станциях и серверах необходимо регулярно обновлять.

24.Администратор системы должен проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратору необходимо выполнить следующие действия: отключить от компьютерной сети рабочие станции, представляющие вирусную опасность до полного выяснения каналов проникновения вирусов и их уничтожения; немедленно сообщить о факте обнаружения вирусов непосредственному начальнику, в том числе указать предположительный источник (отправитель, владелец и т. д.) зараженного файла, тип зараженного файла, тип вируса, а также рассказать о характере содержащейся в файле информации и выполненных антивирусных мероприятиях.

25. Если администратор системы, обрабатывающей персональные данные,подозревает или получил сообщение, что его система подвергается

атаке или уже была скомпрометирована, он должен определить системные ресурсы, безопасность которых была нарушена, а также установить:

была ли попытка несанкционированного доступа (далее - НСД);

когда, как и при каких обстоятельствах была предпринята попытка НСД;

продолжается ли НСД в настоящий момент;

кто является источником НСД;

что является объектом НСД;

какова была мотивация нарушителя;

точку входа нарушителя в систему;

была ли попытка НСД успешной.

26. Для выявления попытки НСД необходимо:

установить, какие пользователи в настоящее время работают в системе и на каких рабочих станциях;

выявить подозрительную активность пользователей, проверить, все ли пользователи вошли в систему со своих рабочих мест и не работает ли кто из них в системе необычно долго;

убедиться, что никто из пользователей не использует подозрительные программы или программы, не относящиеся к его области деятельности.

27. При анализе системных журналов администратор должен:

проверить наличие подозрительных записей в системных журналах,

сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны были отсутствовать в этот период времени, а также входы в систему из неожиданных мест, в необычное время и на короткий период времени;

убедиться в том, что системный журнал не уничтожен и в нем отсутствуют пробелы;

просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;

проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;

проверить журналы на наличие мест, которые выглядят необычно;

выявить неудачные попытки входа в систему.

28. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) следует проверить:

нет ли в них подозрительных записей, сделанных в период предполагаемой попытки НСД;

есть ли в них пробелы, а также места, которые выглядят необычно;

были ли попытки изменения таблиц маршрутизации и адресных таблиц.

Кроме того, необходимо проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

29. Для обнаружения в системе следов, оставленных злоумышленником в виде файлов, вирусов, троянских программ, изменения системной конфигурации следует:

составить базовую схему того, как обычно выглядит система;

провести поиск подозрительных файлов, скрытых файлов, имен файлов и каталогов, которые обычно используются злоумышленниками;

проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;

оценить целостность системных программ;

проверить систему аутентификации и авторизации.

Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

ИНСТРУКЦИЯ

по организации парольной защиты

1.Общие положения

1. Инструкция по организации парольной защиты (далее - Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах образовательного учреждения (далее - ОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее - ИС) ОУ и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора ОУ.

3. Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

пароль должен состоять не менее чем из восьми символов;

- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров,

цифры и специальные символы (@, #, $,&,*, % и т. п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abed и т. д.), общепринятые сокращения (ЭВМ, ЛВС,ШЕК и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

при смене пароля новый пароль должен отличаться от старого не менее чем в шести позициях.

4. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников центра дистанционного образования.

5. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте

или опечатанном пенале передать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для их опечатывания рекомендуется использовать печать отдела кадров.

II. Правила формирования паролей
III. Ввод пароля

6. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

IV. Порядок смены личных паролей

7. Смена паролей проводится регулярно, не реже одного раза в три месяца.

8. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

9. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

10. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 5 Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

11. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

V. Хранение пароля

12. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя подразделения в опечатанном пенале.

13. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

14. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

VI Действия в случае утери и компрометации пароля

15. В случае компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 9 или 10 Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

VII. Ответственность при организации парольной защиты

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

17. Ответственность за организацию парольной защиты в структурных подразделениях ОУ возлагается на системного администратора.

18. Работники ОУ и лица имеющие отношение к обработке персональных данных в информационных системах ОУ, должны быть ознакомлены с Инструкцией под расписку.

Приложение № 5 к разделу IV п.23 Локального акта № 1.12 «Положение об обработке и защите персональных данных» от 18.05.2016 г

ИНСТРУКЦИЯ
пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники

I. Общие положения

1. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (далее - Инструкция), регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) образовательного учреждения (далее - ОУ).

2. Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

II. Обязанности пользователя

3. При выполнении работ в пределах своих функциональных обязанностей пользователь несёт персональную ответственность за соблюдение требований нормативных документов по защите информации.

4. Пользователь обязан:

- выполнять требования Инструкции по обеспечению режима конфиденциальности проводимых работ;
- при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информации была недоступна для просмотра посторонними лицами;
- соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным и файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня производить стирание остаточной информации с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнения" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, меры предотвращения ухудшения ситуации;

- знать и соблюдать правила поведения в экстренных ситуациях, порядок действий при ликвидации последствий аварий;
- помнить личные пароли и персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, администратора системы, а также смежные подразделения, использующие эти файлы в работе;

-оценить необходимость дальнейшего использования файлов, зараженных вирусом;

-провести лечение и уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

6. Пользователю ПЭВМ запрещается:

-записывать и хранить персональные данные на неучтенных в установленном порядке машинных носителях информации;

- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

- самостоятельно подключать к ПЭВМ какие-либо устройства, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;

- самостоятельно устанавливать и/или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

- осуществлять обработку персональных данных в условиях, позволяющих просматривать их лицами, не имеющими к ним допуска, а также нарушающих требования к эксплуатации ПЭВМ;

- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

- отключать (блокировать) средства защиты информации;

- производить какие-либо изменения в подключении и размещении технических средств;

- производить иные действия, ограничения на исполнение которых предусмотрены утверждёнными регламентами и инструкциями;

- бесконтрольно оставлять ПЭВМ с загруженными персональными данными, установленными маркированными носителями, электронными ключами и выведенными на печать документами, содержащими персональные данные.

III. Права пользователя

7. Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;

- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

IV. Заключительные положения

8. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями. 9.Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам и имеющие отношение к обработке персональных данных на объектах вычислительной техники, должны быть ознакомлены с Инструкцией под расписку.

Приложение № 6 к разделу IV п.23 Локального акта № 1.12 «Положение об обработке и защите персональных данных» от 18.05.2016г

Список
работников, допущенных к обработке персональных данных

№ п/п	Ф.И.О. работника	Должность	Дата приема на работу	Адрес, телефон	Примечание

Приложение № 7 к разделу V п.34 Локального акта №1.12 «Положение об обработке и защите персональных данных» от 18.05.2016 г

ИНСТРУКЦИЯ

о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

I. Общие положения

1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее -Инструкция), является обязательной для всех структурных подразделений образовательного учреждения (далее - ОУ).

2. Под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т. ч. его фамилия, ИМЯ, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, доходы и др. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных.

3. В общедоступные источники персональных данных (в т. ч. справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес и другие сведения.

4. Конфиденциальность персональных данных предусматривает обязательное получение согласия субъекта персональных данных (наличие иного законного основания) на их обработку.

Согласие не требуется на обработку данных:

- необходимых для доставки почтовых отправлений организациями почтовой связи;

- включающих в себя только фамилию, имя и отчество субъекта;

- работа с которыми проводится в целях исполнения обращения (запроса) субъекта персональных данных, трудового или иного договора с ним, однократного пропуска в здание или в иных аналогичных целях;

-обработка которых осуществляется без средств автоматизации.

5. Порядок ведения перечней персональных данных в структурных подразделениях ОУ утверждается локальным актом. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

6. Все работники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны иметь допуск (разрешение) к работе с соответствующими видами персональных данных.

7. Работникам, осуществляющим обработку персональных данных, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, а также оставлять материальные носители с персональными данными без присмотра в незапертом помещении. После подготовки и передачи документа в соответствии с резолюцией файлы черновиков и вариантов документа должны переноситься подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

8. Передача персональных данных допускается только в случаях, установленных Федеральными законами от 27.07.2006 № 152-ФЗ "0 персональных данных" и от 02.05.2006 № 59-ФЗ "0 порядке рассмотрения обращений граждан Российской Федерации", действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

9. Запрещается передача персональных данных по телефону, факсу, электронной почте, за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

10. Ответственность за защиту обрабатываемых персональных данных возлагается на работников подразделений ОУ, осуществляющих такую обработку по договору с оператором, а также на иные лица, осуществляющие обработку или хранение конфиденциальных данных в ОУ. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с законодательством РФ и ведомственными нормативными актами.

II. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации

11. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна быть организована таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей персональных данных и установить перечень лиц, осуществляющих обработку.

12. При хранении материальных носителей необходимо соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Лица, осуществляете обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах выполнения такой обработки.

13. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается на одном материальном носителе размещать персональные данные, цели обработки которых заведомо не совместимы. Для обработки персональных данных каждой категории должен использоваться отдельный материальный носитель.

14. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, и невозможности обработки одних персональных данных отдельно от других, зафиксированных на том же носителе, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

15. Уничтожение или обезличивание всех или части персональных данных (если это допускается материальным носителем) производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением ВОЗМОЖНОСТИ обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных 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.

III. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации

16. Безопасность персональных данных при их обработке в информационных системах, хранении и пересылке обеспечивается с помощью системы защиты персональных данных, включающей специальные средства защиты информации, а также используемые в информационной системе информационные технологии.

17. Допуск лиц к обработке персональных данных в информационных системах осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

18. Работа с информационными системами должна быть организована таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключить возможность неконтролируемого пребывания в помещениях, где они находятся, посторонних лиц.

19. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из шести и более символов.

20. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями, а также пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в т. ч. сети Интернет, запрещается.

21. При обработке персональных данных в информационных системах пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

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

постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- недопущение несанкционированного выноса из помещений, установки и подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

22. При обработке персональных данных в информационных системах разработчики и администраторы систем должны обеспечивать:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учёт лиц, допущенных к работе с персональными данными в информационных системах, прав и паролей доступа;

- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;

контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

описание системы защиты персональных данных.

23.Специфические требования к защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

24. Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

Приложение № 8 к разделу VI п.35.2 Локального акта №1.12 «Положение об обработке и защите персональных данных» от 18.05.2016 г

Журнал обращений по ознакомлению с персональными данными.

№ п/п	Ф.И.О. субъекта персональных данных	Дата обращения	Запрашиваемый документ (данные)	Отметка о выполнении	Подпись заявителя	Примечание