Утверждено:
Приказ № 6 от « 13» января 2016 г.

Директор
МБОУ ДО «Гавриловская школа искусств» _____ М.А. Пустотина

ПОЛОЖЕНИЕ
о порядке обработки и защите персональных данных в МБОУ ДО «Гавриловская школа искусств»

1. Общие положения

Настоящее Положение об обработке и защите персональных данных (далее — Положение) в муниципальном бюджетном образовательном учреждении дополнительного образования «Гавриловская школа искусств» (далее – МБОУ ДО «Гавриловская школа искусств») регулирует порядок получения, обработки, использования, хранения и обеспечения конфиденциальности персональных данных в МБОУ ДО «Гавриловская школа искусств» на основании Федерального закона от 27.07.2006 М 152-ФЗ «О персональных данных" (далее — Закон 152-ФЗ), Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", а также в соответствии с уставом МБОУ ДОД «Школа искусств» и локальными актами.

2. Основной задачей МБОУ ДО «Гавриловская школа искусств»в области защиты персональных данных является обеспечение в соответствии с законодательством РФ обработки персональных данных работников МБОУ ДОД «Школа искусств», обучающихся и их родителей (законных представителей), а также персональных данных, содержащихся в документах, полученных из других организаций, обращениях граждан и иных субъектов персональных данных
3. В настоящем Положении используются следующие термины и определения.

Блокирование персональных данных — временное прекращение сбора, систематизации накопления, использования и распространения персональных данных, в т. ч. их передачи.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Информационная система персональных данных — совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием или без использования средств автоматизации.
Информация - любые сведения (сообщения, данные) независимо от формы их представления.

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 распространения без согласия субъекта персональных данных или наличия иного законного основания.
Обеспечения конфиденциальности персональных данных не требуется в случае обезличивания персональных данных и в отношении общедоступных персональных данных.

Обезличивание персональных данных—действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных — действия (операции) с персональными данными: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передача), обезличивание, блокирование, уничтожение персональных данных и др.

Общедоступные персональные данные — персональные данные, на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности или к которым предоставлен доступ неограниченного круга лиц с согласия субъекта персональных данных.
Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных или по решению директора МБОУ ДО «Гавриловская школа искусств», либо по решению суда или иных уполномоченных государственных органов.

Оператор — юридическое лицо (МБОУ ДО «Гавриловская школа искусств»), организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

Персональные данные — любая информация, относящаяся к физическому лицу, определенному или определяемому на основании такой информации, в том числе: его фамилия, имя, отчество; год, месяц, дата и место рождения; адрес регистрации; семейное, социальное и имущественное положение; образование, профессия; доходы; другая информация, определяемая нормативно-правовыми актами РФ в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, настоящим Положением и локальными актами МБОУ ДО «Гавриловская школа искусств».

Работники -лица, имеющие трудовые отношения с МБОУ ДО «Гавриловская школа искусств», либо кандидаты на вакантную должность, вступившие с МБОУ ДО «Гавриловская школа искусств» в отношения по поводу приема на работу.

Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в т. ч. обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Субъекты персональных данных МБОУ ДО «Гавриловская школа искусств» **(далее — субъекты)** — носители персональных данных, в т. ч. работники МБОУ ДО «Гавриловская школа искусств», воспитанники и их родители (законные представители), передавшие свои персональные данные МБОУ ДО «Гавриловская школа искусств»на добровольной основе и (или) в рамках выполнения требований нормативно-правовых актов для их приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в т. ч. передачи) и обезличивания.

Съемные носители данных — материальные объекты или устройства с определенными физическими свойствами, позволяющими использовать их для записи, хранения и считывания персональных данных

.
Типовая форма документа — документ, позволяющий упорядочить, типизировать и облегчить процессы подготовки документов.

Уничтожение персональных данных - действия, в результате которых происходит безвозвратная утрата персональных данных в информационных системах персональных данных, в т.ч. уничтожение материальных носителей персональных данных.

Укрупненный перечень персональных данных - перечень персональных данных субъектов, определенных к обработке оператором в каждом структурном подразделении МБОУ ДОД «Школа искусств».

4. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами РФ, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями МБОУ ДО «Гавриловская школа искусств».
5. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

б. Должностные лица МБОУ ДО «Гавриловская школа искусств», в обязанности которых входит обработка персональных данных субъектов, обеспечивают каждому субъекту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

7. Порядок обработки персональных данных в МБОУ ДО «Гавриловская школа искусств» утверждается директором МБОУ ДО «Гавриловская школа искусств». Все работники МБОУ ДО «Гавриловская школа искусств» должны быть ознакомлены под роспись с настоящим Положением в редакции, действующей на момент ознакомления.

II. Организация получения и обработки персональных данных

8. Получение персональных данных оператором осуществляется в соответствии с нормативно-правовыми актами РФ в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, настоящим Положением, локальными актами МБОУ ДО «Гавриловская школа искусств» в случае согласия субъектов на обработку их персональных данных (приложение 1 к настоящему Положению).

9. Оператор персональных данных не вправе требовать от субъекта предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и частной жизни.

10. Без согласия субъектов осуществляется обработка общедоступных персональных данных или данных, содержащих только фамилии, имена и отчества.

11. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами, а также в случаях, предусмотренных нормативно-правовыми актами РФ и локальными нормативными актами, принятыми в рамках компетенции МБОУ ДОД «Школа искусств» в соответствии с законодательством РФ.

12. В случае увольнения или отчисления субъекта оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено законодательством РФ.

13. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями оператора.

14. Персональные данные хранятся в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях МБОУ ДО «Гавриловская школа искусств» с соблюдением предусмотренных нормативно-правовыми актами РФ мер по защите персональных данных.

15. Право на обработку персональных данных предоставляется работникам МБОУ ДО «Школа искусств», определенным укрупненным перечнем персональных данных, используемых работниками структурных подразделений и (или) должностными лицами МБОУ ДО «Гавриловская школа искусств» , а также распорядительными документами и иными письменными указаниями оператора.

16. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в укрупненный перечень персональных данных, используемых работниками структурных подразделений и (или) должностными лицами МБОУ ДО «Гавриловская школа искусств», запрещается.

17. Работники структурных подразделений и (или) должностные лица МБОУ ДО «Гавриловская школа искусств», проводящие сбор персональных данных на основании укрупненного перечня, обязаны сохранять их конфиденциальность.

18. Персональные данные при их обработке обособляются от иной информации, в частности путем фиксации их на отдельных материальных (бумажном или электронном) носителях персональных данных (далее — материальные носители), в специальных разделах или на полях форм (бланков).

19. При фиксации персональных данных на материальных носителях не допускается размещение на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.
для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, применяются отдельные материальные носители для каждой категории.

20.Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в т. ч. работники МБОУ ДО «Гавриловская школа искусств» или лица, осуществляющие такую обработку по договору с МБОУ ДО «Гавриловская школа искусств»), информируются руководителями:
• о факте обработки ими персональных данных;
• категориях обрабатываемых персональных данных;
• об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, а также локальными актами МБОУ ДО «Гавриловская школа искусств»
21. При использовании типовых форм документов (приложение 2 к настоящему Положению), характер информации в которых предполагает или допускает включение в них персональных данных (далее — типовая форма), должны соблюдаться следующие условия:
• типовая форма документа содержит сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; наименование МБОУ ДО «Гавриловская школа искусств»; адрес МБОУ ДО «Гавриловская школа искусств»; 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 МБОУ ДО «Гавриловская школа искусств» способов обработки персональных данных;
• при необходимости получения письменного согласия на обработку персональных данных типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации;
типовая форма составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, не нарушая прав и законных интересов иных субъектов персональных данных.

22. При ведении журналов (журналов регистрации, журналов посещений и др.), содержащих персональные данные субъектов, следует учитывать, во-первых, что необходимость их ведения предусмотрена федеральными законами и локальными актами МБОУ ДО «Гавриловская школа искусств», содержащими сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способах фиксации и составе информации, запрашиваемой у субъектов персональных данных, перечне лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журналов, сроках обработки персональных данных, и, во-вторых, что копирование содержащейся в них информации не допускается.

23. Уничтожение или обезличивание 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, зачеркивание, стирание)

24. 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.

25. Если персональные данные субъекта можно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него необходимо получить письменное согласие. МБОУ ДО «Гавриловская школа искусств» должна сообщить субъекту

о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта представить письменное согласие на их получение.

III. Меры по обеспечению безопасности персональных данных при их обработке

26. При обработке персональных данных в отношении каждой категории персональных данных определяются места хранения, а также устанавливается перечень лиц, осуществляющих их обработку либо имеющих к ним доступ (как с использованием средств автоматизации, так и без них).

27. Оператором обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

28. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе управленческой и производственной деятельности МБОУ ДО «Гавриловская школа искусств».

29. Порядок конкретных мероприятий по защите персональных данных с использованием или без использования ПК определяется приказами директора МБОУ ДО «Гавриловская школа искусств» и иными локальными нормативными актами.

IV. Права, обязанности и ответственность субъекта персональных данных и оператора при обработке персональных данных

30. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Законом 152-ФЗ за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

• на получение сведений об операторе, о месте его нахождения, наличии у него персональных данных, относящихся к нему (т. е. субъекту персональных данных), а также на ознакомление с такими данными;

• требование от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

• получение при обращении или запросе информации, касающейся обработки его персональных данных.

31. Оператор обязан:

• безвозмездно предоставлять субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных;

• вносить в персональные данные субъекта необходимые изменения;

• уничтожать или блокировать соответствующие персональные данные при предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

• уведомлять субъекта персональных данных или его законного представителя и третьих лиц,

которым персональные данные этого субъекта были переданы, о внесенных изменениях и предпринятых мерах;
• в случае выявления неправомерных действий с персональными данными субъекта устранять допущенные нарушения в срок, не превышающий трех рабочих дней с даты такого выявления;
• в случае невозможности устранения допущенных нарушений уничтожать персональные данные субъекта в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными;
• уведомлять субъекта персональных данных или его законного представителя об устранении допущенных нарушений или об уничтожении персональныхданных;
• в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных;
• уведомить субъекта персональных данных об уничтожении его персональных данных.

32. Оператор не вправе без письменного согласия (приложение 3 к настоящему Положению) субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством РФ.

33. Ответственность за соблюдение требований законодательства РФ при обработке и использовании персональных данных возлагается на руководителей структурных подразделений и конкретных должностных лиц, обрабатывающих персональные данные, в приказе об утверждении настоящего Положения и в других соответствующих приказах.

V. Заключительные положения

34. Изменения в Положение вносятся согласно установленному в МБОУ ДО «Гавриловская школа искусств» порядку. Право ходатайствовать о внесении изменений в Положение имеет директор МБОУ ДО «Гавриловская школа искусств».

Утверждена:
приказом №6 от «13 января 2016 г.

Директор
МБОУ ДО «Гавриловская школа искусств» _____ Пустотина М.А

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

1. Общие положения

1.1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее — Инструкция), является обязательной для всех структурных подразделений МБОУ ДО «Гавриловская школа искусств»
1.2. 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.
1.3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных. 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.
1.4. Конфиденциальность персональных данных предусматривает обязательное получение согласия субъекта персональных данных (наличие иного законного основания) на их обработку. Согласие не требуется на обработкуданных:
• необходимых для доставки почтовых отправлений организациями почтовой связи;
• включающих в себя только фамилию, имя и отчество субъекта;
• данных, 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.
1 .5. Порядок ведения перечней персональных данных в структурных подразделениях МБОУ ДО «Школа искусств» утверждается локальным актом. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.
1 .6. Все работники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны иметь допуск (разрешение) к работе с соответствующими видами персональных данных.
1 .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.
1 .8. Передача персональных данных допускается только в случаях, установленных Федеральными законами от 27.07.2006 ‘Ф 1 52-ФЗ “О персональных данных” и от 02.05.2006 Г 59-ФЗ “О 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.
1.9. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством РФ 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.
1.10. Ответственность за защиту обрабатываемых персональных данных возлагается на работников подразделений МБОУ ДО «Гавриловская школа искусств», осуществляющих такую обработку по договору с оператором, а также на иные лица, осуществляющие обработку или хранение конфиденциальных данных в МБОУ ДО «Гавриловская школа искусств». Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами.

2. Порядок обеспечения безопасности при обработке и хранении персо-. нальных данных, осуществляемых без использования средств автоматизации
2.1. 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.
2.2. При хранении материальных носителей необходимо соблюдать условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Лица, осуществляющие 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.
2.3. 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.
2.4. 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.
2.5. 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.
3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации
3.1. 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.
3.2. допуск лиц к обработке персональных данных в информационных системах

осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

3.3. 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.

3.4. 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.

3.5. 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.

3.6. 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.

3.7. 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;

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

• учет 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.

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

3.9. Работники подразделений МБОУ ДО «Гавриловская школа искусств» и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку

Утверждена:
приказом №6 от «13 января 2016 г.

Директор
МБОУ ДО «Гавриловская школа искусств» _____ Пустотина М.А

Инструкция
пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники

1. Общие положения

1.1. 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 и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) МБОУ ДО «Гавриловская школа искусств»
1.2. Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

2. Обязанности пользователя

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

2.2. Пользователь обязан:

• выполнять требования Инструкции по обеспечению режима конфиденциальных проводимых работ;

• при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемо информации лиц, а также располагать во время работы экран видеомонитор 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, файлам с персональными данными при ее обработке;
• после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня стирать остаточную информацию с жесткого диска ПЭВМ;
• оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководитель обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

• не допускать 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.

2.3. 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 или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

2.4. 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 лицам, не имеющим 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 утвержденными регламентами и инструкциями;

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

2. Права пользователя

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.

3. Заключительные положения

3.1. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.
3.2. Работники подразделений МБОУ ДО «Гавриловская школа искусств» 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.

Утверждена:
приказом №6 от «13 января 2016 г.

Директор
МБОУ ДО «Гавриловская школа искусств» _____ Пустотина М.А

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 МБОУ ДО «Гавриловская школа искусств»
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 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.
7. 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.
8. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности, и включают:
• составление отчетов 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, 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 1. СО 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 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 необходимо применять антивирусное программное обеспечение, позволяющее осуществлять проверку всех входящих сообщений. В случае если проверка входящего сообщения 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 т. ч. 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 о том, что его система подвергается атаке или уже была скомпрометирована, он должен определить системные ресурсы, безопасность которых была нарушена, и 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.

30. Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.
31. Работники подразделений ДОУ 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.

Утверждена:
приказом №6 от «13 января 2016 г.

Директор
МБОУ ДО «Гавриловская школа искусств» _____ Пустотина М.А

Инструкция
по организации парольной защиты

1. Общие положения

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 МБОУ ДО «Гавриловская школа искусств», а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.
1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее — ИС) МБОУ ДО «Гавриловская школа искусств» контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора МБОУ ДО «Гавриловская школа искусств» .

2. Правила формирования паролей

2.1. 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 (@,, $, 8, , % 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, gwerty, aЬocd и т. д.), общепринятые сокращения (ЭВМ, ЛВС, 1.)ЗЕЯ 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.
2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников центра дистанционного образования.
2.3. 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.

3. Ввод пароля

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.).

4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, не **реже** одного раза в три месяца.
4.2. 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.
4.3. 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.
4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.1 Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).
4.5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

5. Хранение пароля

5.1. 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.
5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.
5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. действия в случае утери и компрометации пароля

В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 4.3 или п. 4.4 Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.
7.2. Ответственность за организацию парольной защиты в структурных подразделениях МБОУ ДО «Гавриловская школа искусств» возлагается на системного администратора.
7.3. Работники МБОУ ДО «Гавриловская школа искусств» и лица, имеющие отношение к обработке персональных данных в информационных системах МБОУ ДО «Гавриловская школа искусств», должны быть ознакомлекы с Инструкцией под расписку.

Нормативные документы

• Федеральный закон от 23.12.2010 Г 359-ФЗ «О внесении изменения в статьи Федерального закона “О персональных данных”«
• Федеральный закон от 27.07.2006 152-ФЗ “О персональных данных” (реа 23.12.2010)
• Федеральный закон от 27.07.2006 Г<] 149-ФЗ “Об информации, информацис технологиях и о защите информации” (ред. от 06.04.2011)
• Федеральный закон от 02.05.2006 Г] 59-ФЗ порядке рассмотрения обращ граждан Российской Федерации” (ред. от 27.07.201 0)