Муниципальное бюджетное учреждение дополнительного образования
«Каневская районная детская школа искусств»
муниципального образования Каневской район
(МБУ ДО «Каневская РДШИ»)

УТВЕРЖДЕНО
приказом по основной
деятельности
МБУ ДО «Каневская РДШИ»
от 28.08.2019г. № 110

ПОЛОЖЕНИЕ №55
о постоянно действующей комиссии по защите персональных данных

Положение о постоянно действующей комиссии по защите персональных данных определяет особенности формирования и функционирования постоянно действующей комиссии по защите персональных данных в МБУ ДО «Каневская РДШИ».

Все лица, назначенные приказом директора в состав постоянно действующей комиссии по защите персональных данных, в обязательном порядке должны быть ознакомлены с настоящим положением под подпись.

Положение вступает в силу с момента утверждения приказом директора.

Положение бессрочно до замены или отмены.

Все изменения вносятся приказом директора.

Пересмотр положений данного положения осуществляется по мере необходимости, но не реже одного раза в три года.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ.

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. Выделенные помещения – помещения (кабинеты, актовые и выставочные залы и т.д.) специально предназначенные для обработки персональных данных.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями

правовых документов или требованиями, устанавливаемыми собственником информации.

Информационная безопасность (организации) – состояние защищенности интересов организации в условиях угроз в информационной сфере.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (Федеральный закон от 27.07.2006 № 149-ФЗ).

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Непреднамеренное воздействие на информацию – ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированный доступ (к информации) – доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации.

Носитель информации – материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

Оператор (персональных данных) –юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие

цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Федеральный закон от 27.07.2006 № 152-ФЗ).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ).

Правило доступа (к защищаемой информации) – совокупность правил, регламентирующих порядок и условия доступа субъекта к защищаемой информации и ее носителям.

Право доступа (к защищаемой информации) – совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.

Система защиты персональных данных – совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах персональных данных.

Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ).

Угроза информационной безопасности (организации) – совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

Комиссия – постоянно действующая комиссия по защите персональных данных;

ЛНА – локальные нормативные акты;

НСД – несанкционированный доступ;

ПДн – персональные данные;
ПО – программное обеспечение;
СЗИ – средство защиты информации;
СЗПДн – система защиты персональных данных;
ТС – технические средства;
УБПДн – угроза безопасности персональных данных;
Учреждение/организация – МБУ ДО «Каневская РДШИ».

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Комиссия создается в целях исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О ПДн» и принятых в соответствии с ним нормативных правовых актов, а также организации процессов обработки и защиты ПДн в Учреждении.

3.2. Структура, численность и персональный состав Комиссии определяются приказом директора с учетом требований настоящего положения.

3.3. В состав Комиссии могут быть включены наиболее квалифицированные и ответственные работники Учреждения, а также приглашенные специалисты и эксперты сторонних организаций, компетентные в соответствующих областях знаний.

3.4. Комиссия действует на постоянной основе и подчиняется директору.

4. СОСТАВ КОМИССИИ

4.1. Комиссия состоит из председателя Комиссии и членов Комиссии. Из числа членов Комиссии назначаются заместитель председателя Комиссии и секретарь Комиссии.

4.2. Руководство Комиссией осуществляет председатель Комиссии.

4.2.1. Председатель Комиссии является ответственным должностным лицом Учреждения за организацию СЗПДн, ее обеспечение и поддержание функционирования, выполнение возложенных на Комиссию задач и функций.

4.2.2. Председатель Комиссии планирует и организует работу Комиссии, председательствует на заседаниях Комиссии, распределяет обязанности между членами Комиссии, дает им поручения. По результатам распределения обязанностей формируется перечень обязанностей членов Комиссии.

4.2.3. Председатель Комиссии назначает ответственных должностных лиц из числа членов Комиссии за решение отдельных вопросов в различных направлениях деятельности Комиссии.

4.2.4. Председатель Комиссии определяет место, время и утверждает повестку дня заседания Комиссии.

4.2.5. Председатель Комиссии организует работу по подготовке проектов ЛНА, по внесению изменений в состав Комиссии в связи с организационно-кадровыми изменениями в течение 14 дней с момента их возникновения, по внесению изменений и дополнений в настоящее положение, по реорганизации и упразднению Комиссии.

4.2.6. Председатель Комиссии осуществляет контроль реализации принятых Комиссией решений и рекомендаций и представляет Комиссию по вопросам, относящимся к ее компетенции.

4.2.7. В случае временного отсутствия председателя Комиссии или невозможности временно исполнять возложенные на него функции, в срок не позднее 10 дней с момента возникновения таких обстоятельств, заместитель председателя Комиссии принимает на себя функции по организации СЗПДн, ее обеспечению и поддержанию функционирования. Заместитель председателя Комиссии организует деятельность членов Комиссии по порученным ему направлениям, организует участие в заседаниях Комиссии представителей заинтересованных органов государственной власти и организаций.

4.3. Члены Комиссии подбираются на основании уровня их компетентности в вопросах защиты ПДн, а также осведомленности о структуре Учреждения.

4.3.1. Члены Комиссии имеют право вносить председателю Комиссии предложения по формированию повестки дня заседания Комиссии и плана работы Комиссии в целом.

4.3.2. Секретарь Комиссии отвечает за подготовку заседаний Комиссии, сбор и подготовку материалов к заседаниям Комиссии, подготовку проектов планов работы Комиссии, формирует проект повестки дня заседания Комиссии, оформляет протоколы заседаний Комиссии, готовит отчеты о работе Комиссии, информирует членов Комиссии о месте, времени и о повестке дня очередного заседания Комиссии и обеспечивает их необходимыми справочно-информационными материалами, формирует в дела документы Комиссии, хранит их и сдает в архив в установленном порядке.

5. ДЕЯТЕЛЬНОСТЬ КОМИССИИ

5.1. Комиссия в своей деятельности руководствуется:

- настоящим положением;

- положением о защите, хранении, обработке и передаче персональных данных работников, обучающихся и их родителей (законных представителей);
- положением о разграничении прав доступа к обрабатываемым персональным данным
- регламентом проведения внутренних мероприятий по контролю обеспечения защиты ПДн;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О ПДн»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите ПДн при их обработке в ИСПДн»;
- постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»;
- методическими и нормативными документами ФСТЭК России и ФСБ России в области защиты ПДн;
- ЛНА Учреждения, регламентирующими обработку и защиту ПДн;
- прочими Федеральными законами, указами Президента РФ, постановлениями Правительства РФ и иными нормативными правовыми актами, регламентирующими обработку и защиту ПДн в РФ.

5.2. Деятельность Комиссии организуется и проводится в соответствии с перспективными и текущими планами работы, в которые включаются мероприятия, предусматривающие следующие основные направления:

- анализ деятельности Учреждения в вопросах обработки и защиты ПДн за отчетный период;
- общий контроль организации защиты ИСПДн Учреждения;
- подготовка рекомендаций, направленных на обеспечение СЗПДн.

5.3. Планы работы Комиссии формируются под руководством председателя или заместителя председателя Комиссии и утверждаются директором. При необходимости, вопросы, не нашедшие отражения в планах работы Комиссии, могут быть вынесены на рассмотрение Комиссии во внеплановом порядке.

5.4. Всем членам Комиссии предоставляется допуск к ПДн в объеме, необходимом для исполнения своих обязанностей и функций в качестве членов Комиссии.

6. ЗАСЕДАНИЯ КОМИССИИ

6.1. Заседания Комиссии проводятся по мере необходимости.

6.2. Внеочередные заседания Комиссии проводятся по решению председателя Комиссии.

6.3. При необходимости, на заседания Комиссии могут приглашаться специалисты и эксперты сторонних организаций, компетентные в предметных областях.

6.4. Заседание Комиссии считается правомочным, если на нем присутствует не менее половины ее членов.

6.5. Рассмотрение вопросов, выносимых на заседание Комиссии, не должно приводить к необоснованному расширению круга лиц, допускаемых к сведениям по рассматриваемой тематике. Доступ приглашенных компетентных специалистов и экспертов к таким сведениям осуществляется в соответствии с распоряжением директора, а их присутствие на заседаниях Комиссии ограничивается рассмотрением вопросов, для обсуждения которых они приглашены.

6.6. По результатам обсуждения на заседании запланированных вопросов Комиссия принимает решения большинством голосов.

6.7. По результатам заседаний Комиссии оформляются протоколы, которые подписываются председателем (заместителем председателя) и другими членами Комиссии.

6.8. Члены Комиссии, в случае несогласия с принятым на заседании Комиссии решением, имеют право письменно изложить свое особое мнение, которое подлежит обязательному приобщению к протоколу заседания.

7. ЗАДАЧИ КОМИССИИ

7.1. Основными задачами Комиссии являются:

- разработка единой концепции обеспечения безопасности ПДн в Учреждении, определение требований к СЗПДн и документообороту на бумажных и машинных носителях информации;
- планирование и организация мероприятий, и координация работ по обеспечению безопасности ПДн на всех этапах их обработки; определение необходимости обеспечения установленных Правительством РФ уровней защищенности ПДн при их обработке в ИСПДн;
- контроль и оценка эффективности принимаемых мер защиты ПДн и применяемых СЗИ; организация и проведение учебно-методических мероприятий с работниками Учреждения по вопросам защиты ПДн;

- обеспечение законности и правомерности обработки ПДн в Учреждении, а также свободной реализации прав и интересов субъектов ПДн.

8. ФУНКЦИИ КОМИССИИ

8.1. С целью эффективного решения поставленных задач Комиссия выполняет следующие функции:

Организационные:

- формирует перечень обрабатываемых ПДн, проводит их категорирование, определяет сроки хранения и порядок уничтожения носителей ПДн;
- формирует списки лиц, допущенных к обработке ПДн, в выделенные помещения, к информационным ресурсам и ИСПДн в целом;
- организует и обеспечивает порядок доступа в выделенные помещения;
- принимает решение об использовании в Учреждении сертифицированных программных, аппаратных, программно-аппаратных и криптографических СЗИ;
- анализирует и прогнозирует ситуации в области защиты ПДн, в том числе проводит анализ возможных УБПДн и каналов их утечки, прогнозирует появления новых еще не известных угроз, разрабатывает предложения по их предотвращению;
- анализирует и прогнозирует изменение нормативных правовых актов и требований законодательства РФ в области ПДн;
- создает условия и механизмы оперативного реагирования на УБПДн. составляет акты и другую техническую документацию о степени защищенности выделенных помещений, АРМ и ИСПДн в целом. Планирует и организует практические мероприятия по предотвращению попыток несанкционированного вмешательства в процессы нормального функционирования ИСПДн и попыток НСД к обрабатываемым ПДн. Создает условия для максимально возможного возмещения ущерба и локализации негативных последствий, возникших в результате неправомерных действий физических лиц или случайных событий, ослабления последствий нарушения безопасности ПДн;
- принимает мотивированные решения о передаче ПДн субъектов ПДн или о предоставлении к ним доступа третьим лицам или сторонним организациям;
- принимает решения о необходимости привлечения сторонних специализированных организаций для выполнения отдельных работ,

связанных с модернизацией и (или) аудитом СЗПДн, ремонтом ТС ИСПДн и др.;

- осуществляет подготовку к организуемым контролирующими органами мероприятиям по контролю защиты ПДн в Учреждении;
- доводит до сведения работников Учреждения требования законодательства РФ в области ПДн, а также требования ЛНА Учреждения, регламентирующих обработку и защиту ПДн;
- организует и проводит занятия с работниками Учреждения по вопросам защиты ПДн, правилам работы в ИСПДн и изучению ЛНА, регламентирующих обработку и защиту ПДн;
- планирует свою деятельность.

Контрольные:

- принимает участие в проектировании, приемке, сдаче в эксплуатацию программных средств и автоматизированных систем Учреждения (в части требований к обеспечению безопасности ПДн);
- организует контроль над выполнением специальных требований по размещению ТС ИСПДн;
- организует и проводит работы по контролю наличия материальных носителей ПДн, экспертизе ценности документов, условий их хранения и уничтожения;
- контролирует соблюдение требований технических условий, правил эксплуатации и сертификатов на эксплуатируемые СЗИ;
- контролирует полноту и своевременность выполнения мероприятий по защите ПДн и принятых решений Комиссии;
- контролирует функционирование СЗПДн и подготавливает предложения по ее совершенствованию;
- обеспечивает соответствие проводимых работ по защите ПДн технике безопасности, правилам и нормам охраны труда.

Технические:

- организует и контролирует проектирование, разработку, внедрение, установку, настройку, администрирование и удаление СЗИ и СЗПДн в целом;
- организует и проводит мероприятия по очистке и (или) уничтожению машинных носителей ПДн.

Специальные:

- проводит служебные расследования по фактам нарушения безопасности ПДн, в том числе анализирует обстоятельства и причины такого нарушения, определяет реальный и потенциальный ущерб для Учреждения и (или) субъекта ПДн;

- проводит анализ и расследование инцидентов ИБ, вырабатывает стратегии устранения последствий подобных инцидентов, а также требования и рекомендации по их предупреждению и устранению в будущем.

9. ПОЛНОМОЧИЯ КОМИССИИ

9.1. Комиссия имеет право:

- знакомиться с документами и материалами, необходимыми для выполнения возложенных задач и функций;
- выступать с инициативой по разработке проектов ЛНА, регламентирующих обработку и защиту ПДн в Учреждении;
- давать работникам Учреждения обязательные для выполнения указания по защите ПДн, определяемые действующим законодательством РФ и ЛНА Учреждения;
- принимать мотивированные решения о привлечении сторонних специализированных организаций к проведению работ по технической защите ПДн;
- привлекать в установленном порядке работников Учреждения, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе своей работы, и выработки обоснованных рекомендаций и заключений;
- привлекать лицо, ответственное за обеспечение работоспособности ПО и ТС ИСПДн к выполнению работ по установке, настройке, администрированию и удалению СЗИ, а также к администрированию СЗПДн;
- проводить проверки соблюдения установленного порядка защиты ПДн;
- вносить предложения о приостановке действий, противоречащих законодательству РФ в области ПДн, по направлениям, отнесенным к компетенции Комиссии;
- принимать необходимые меры в случае обнаружения нарушения установленного порядка защиты ПДн, вплоть до приостановки обработки ПДн в ИСПДн в Учреждении в целом;
- требовать от работников Учреждения письменных объяснений необходимых обстоятельств и фактов при проведении служебных расследований;
- подготавливать и представлять в установленном порядке предложения о порядке определения размера ущерба, который может быть причинен Учреждению, его работникам либо субъектам ПДн вследствие нарушения безопасности ПДн;

- вносить предложения об отстранении от выполнения служебных (трудовых) обязанностей работников Учреждения, систематически нарушающих требования по защите ПДн;
- являться инициатором применения мер дисциплинарного взыскания по отношению к работникам, нарушающим установленный порядок защиты ПДн.

9.2. Членам Комиссии запрещается:

- доводить до работников Учреждения сведения о СЗПДн в полном объеме;
- при выводе из состава Комиссии раскрывать объем работ и конкретные направления деятельности Комиссии, разглашать информацию, ставшую известной в ходе работы в составе Комиссии.

10. СВОДНЫЙ ПЕРЕЧЕНЬ РЕГУЛЯРНЫХ МЕРОПРИЯТИЙ

5.1. Сводный перечень регулярных мероприятий, вводимых настоящим положением, представлен в таблице ниже, в которой для каждого мероприятия указаны:

- наименование;
- периодичность выполнения;
- номер пункта настоящего документа, вводящего мероприятие;
- ответственное за выполнение мероприятия лицо.

Таблица – сводный перечень регулярных мероприятий

Наименование мероприятия	*Периодичность*	*Ответственный*
Заседание комиссии и оценка эффективности принимаемых мер защиты ПДн	Ежегодно	Гончар Н.Н.
Организация и проведение учебно-методических мероприятий с работниками Учреждения по вопросам защиты ПДн	Ежегодно	Мартынюк В.Ф. Глушко М.Ю.
Контроль порядка доступа в выделенные помещения	Ежегодно	Краева С.А.
Анализ возможных УБПДн и каналов их утечки	Ежегодно	Панченко Т.И.
Контроль соблюдения требований технических условий, правил эксплуатации и	Ежегодно	Краева С.А.

сертификатов на эксплуатируемые СЗИ		
Планирование и организация практических мероприятий по предотвращению попыток несанкционированного вмешательства в процесс нормального функционирования ИСПДн и попыток НСД к обрабатываемым ПДн	Ежегодно	Гончар Н.Н.
Контроль полноты и своевременности выполнения мероприятий по защите ПДн	Ежегодно	Панченко Т.И.

5.2. Председатель Комиссии несет персональную ответственность за деятельность Комиссии, качество и своевременность исполнения обязанностей, возложенных на него в соответствии с настоящим положением и перечнем обязанностей членов Комиссии.

5.3. Председатель Комиссии несет персональную ответственность за поддержание установленных уровней защищенности ПДн при их обработке в ИСПДн Учреждения, а также заданного уровня ИБ Учреждения.

5.4. Члены Комиссии несут персональную ответственность за качество и своевременность исполнения обязанностей, возложенных на них в соответствии с настоящим положением и перечнем обязанностей членов Комиссии.

11. ОБЯЗАННОСТИ ЧЛЕНОВ ПОСТОЯННО ДЕЙСТВУЮЩЕЙ КОМИССИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Обязанности членов постоянно действующей комиссии по защите персональных данных:

- организация системы защиты персональных данных, ее обеспечение и поддержание функционирования;
- координация деятельности по реализации мероприятий по защите персональных данных;
- реализация мероприятий по защите персональных данных;
- организация и проведение внутренних мероприятий (проверок) по контролю обеспечения защиты персональных данных;

- подготовка ответов на обращения (запросы) субъектов персональных данных, правоохранительных и дознавательных органов;
- повседневный контроль соблюдения требований по обеспечению безопасности персональных данных;
- ознакомление работников с локальными нормативными актами, регламентирующими защиту и обработку персональных данных Организация и проведение учебно-методических мероприятий по вопросам защиты персональных данных;
- разъяснение субъектам персональных данных их прав, положений законодательства РФ в области персональных данных;
- реагирование на нештатные и чрезвычайные ситуации;
- хранение, учет, использование и уничтожение машинных носителей информации, предназначенных для обработки персональных данных;
- хранение, учет ключей от выделенных помещений, сейфов, шкафов, предназначенных для обработки персональных данных;
- анализ и оценка возможных угроз безопасности персональных данных и каналов их утечки, при их обработке в информационных системах персональных данных.

СОГЛАСОВАНО
Протокол заседания общего собрания трудового коллектива
МБУ ДО «Каневская РДШИ»
от 28.08.2019г. № 6