УТВЕРЖДЕНО
приказом ГПОУ «УМК»
от 31.08.2016 № 42

ПОЛОЖЕНИЕ

о постоянно действующей комиссии по защите персональных данных

Содержание

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Назначение документа

Положение о постоянно действующей комиссии по защите персональных данных определяет особенности формирования и функционирования постоянно действующей комиссии по защите персональных данных в ГПОУ «УМК».

Цели принятия

Формализация порядка назначения и работы, состава, обязанностей, полномочий и ответственности постоянно действующей комиссии по защите персональных данных.

Область применения

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.

Вступление в силу

С момента утверждения директором. Действует бессрочно до замены или отмены.

Все изменения вносятся приказом директора. Пересмотр осуществляется по мере необходимости, но не реже одного раза в три года.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

База данных – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ (ГОСТ 20886-85).

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность (ГОСТ Р 50922-2006).

Выделенные помещения – помещения (кабинеты, актовые, конференц-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 (ГОСТ Р 50922-2006).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922-2006).

Информационная безопасность (организации) – состояние защищенности интересов организации в условиях угроз в информационной сфере (ГОСТ Р 53114-2008).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ).

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 (ГОСТ Р ИСО/МЭК 27001-2006).

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 (ГОСТ Р 51583-2000[1]).

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 (ГОСТ Р 50922-2006).

---

[1] Заменен на ГОСТ Р 51583-2014 (с 1 сентября 2014 г.)

Несанкционированный доступ (к информации) – доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации (Р 50.1.053-2005).

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 (ГОСТ Р 50922-2006).

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) – государственный орган, муниципальный орган, юридическое или физическое 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 (ГОСТ Р 50922-2006).

Право доступа (к защищаемой информации) – совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации (ГОСТ Р 50922-2006).

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации (ГОСТ Р 53114-2008).

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 (Постановление Правительства РФ от 01.11.2012 № 1119).

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 (ГОСТ Р 53114-2008).

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками (ГОСТ Р 53114-2008).

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	– ГПОУ «УМК».

1.2.3.7. 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. Передача возложенных обязательств оформляется приказом директора.

1.2.4. Члены Комиссии

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

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

1.2.4.3. Заместитель председателя Комиссии по поручению председателя Комиссии исполняет его обязанности в момент отсутствия. Заместитель председателя Комиссии организует деятельность членов Комиссии по порученным ему направлениям, организует участие в заседаниях Комиссии представителей заинтересованных органов государственной власти и организаций.

1.2.4.4. 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.

2.2.1. Заседания Комиссии проводятся по мере необходимости, но не реже одного раза в полгода.

2.2.2. Внеочередные заседания Комиссии проводятся по решению председателя Комиссии.

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

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

2.2.5. 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.

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

2.2.7. По результатам заседаний Комиссии оформляются протоколы, которые подписываются председателем (заместителем председателя) и другими членами Комиссии и представляются директору на ознакомление.

2.2.8. 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.

2.3. Отчетность

2.3.1. Комиссия подотчетна директору.

2.3.2. Председатель Комиссии периодически, но не реже одного раза в год, представляет директору отчет об итогах работы Комиссии и реализации ее предложений и рекомендаций.

2.3.3. Отчет об итогах работы Комиссии за истекший год представляется на рассмотрение директору не позднее одного месяца после окончания календарного года.

2.3.4. Кроме отчета об итогах работы Комиссии директору могут быть представлены:

- информационные материалы о состоянии ИБ Учреждения;
- предложения по решению актуальных проблем обеспечения защиты ПДн в Учреждении, в том числе по совершенствованию СЗПДн;
- предложения по внесению изменений и дополнений в ЛНА Учреждения, регламентирующие обработку и защиту ПДн.

3.2.1.1.8. Создает условия и механизмы оперативного реагирования на УБПДн.

3.2.1.1.9. Составляет акты и другую техническую документацию о степени защищенности выделенных помещений, АРМ и ИСПДн в целом.

3.2.1.1.10. Планирует и организует практические мероприятия по предотвращению попыток несанкционированного вмешательства в процессы нормального функционирования ИСПДн и попыток НСД к обрабатываемым ПДн.

3.2.1.1.11. 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.

3.2.1.1.12. Принимает мотивированные решения о передаче ПДн субъектов ПДн или о предоставлении к ним доступа третьим лицам или сторонним организациям.

3.2.1.1.13. Принимает решения о необходимости привлечения сторонних специализированных организаций для выполнения отдельных работ, связанных с модернизацией и (или) аудитом СЗПДн, ремонтом ТС ИСПДн и др.

3.2.1.1.14. Осуществляет подготовку к организуемым контролирующими органами мероприятиям по контролю защиты ПДн в Учреждении.

3.2.1.1.15. Доводит до сведения работников Учреждения требования законодательства РФ в области ПДн, а также требования ЛНА Учреждения, регламентирующих обработку и защиту ПДн.

3.2.1.1.16. Организует и проводит занятия с работниками Учреждения по вопросам защиты ПДн, правилам работы в ИСПДн и изучению ЛНА, регламентирующих обработку и защиту ПДн.

3.2.1.1.17. Осуществляет ведение журналов учета СЗПДн.

3.2.1.1.18. Принимает и обрабатывает обращения и запросы субъектов ПДн и (или) контролирует прием и обработку таких обращений и запросов в Учреждении.

3.2.1.1.19. Планирует свою деятельность.

3.2.1.2. Контрольные:

3.2.1.2.1. Принимает участие в проектировании, приемке, сдаче в эксплуатацию программных средств и автоматизированных систем Учреждения (в части требований к обеспечению безопасности ПДн).

3.2.1.2.2. Организует контроль над выполнением специальных требований по размещению ТС ИСПДн, прокладке кабельных трасс и инженерных систем, организации резервного копирования ПДн, а также созданию и использованию эталонных копий ПО в части обеспечения безопасности ПДн и процессов их обработки.

3.2.1.2.3. Организует и проводит работы по контролю наличия материальных носителей ПДн, экспертизе ценности документов, условий их хранения и уничтожения.

3.2.1.2.4. Контролирует соблюдение требований технических условий, правил эксплуатации и сертификатов на эксплуатируемые СЗИ.

3.2.1.2.5. Контролирует полноту и своевременность выполнения мероприятий по защите ПДн и принятых решений Комиссии в структурных подразделениях Учреждения.

3.2.1.2.6. Осуществляет периодический контроль системных журналов СЗИ.

3.2.1.2.7. Проводит экспертизу договоров Учреждения со сторонними организациями по вопросам обеспечения безопасности ПДн.

3.2.1.2.8. Организует и контролирует выполнение плановых заданий, договорных обязательств, а также сроков, полноты и качества работ, выполняемых соисполнителями.

3.2.1.2.9. Контролирует функционирование СЗПДн и подготавливает предложения по ее совершенствованию.

3.2.1.2.10. Обеспечивает соответствие проводимых работ по защите ПДн технике безопасности, правилам и нормам охраны труда.

3.2.1.3. Технические:

3.2.1.3.1. Организует и контролирует проектирование, разработку, внедрение, установку, настройку, администрирование и удаление СЗИ и СЗПДн в целом.

3.2.1.3.2. Организует и проводит мероприятия по очистке и (или) уничтожению машинных носителей ПДн.

3.2.1.4. Специальные:

3.2.1.4.1. 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.

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

4. Полномочия Комиссии

4.1. Комиссия имеет право:

4.1.1. Знакомиться с документами и материалами, необходимыми для выполнения возложенных задач и функций.

4.1.2. Выступать с инициативой по разработке проектов ЛНА, регламентирующих обработку и защиту ПДн в Учреждении.

4.1.3. Давать работникам Учреждения обязательные для выполнения указания по защите ПДн, определяемые действующим законодательством РФ и ЛНА Учреждения.

4.1.4. Принимать мотивированные решения о привлечении сторонних специализированных организаций к проведению работ по технической защите ПДн.

4.1.5. Организовывать и координировать работу всех структурных подразделений Учреждения в вопросах обработки и защиты ПДн.

4.1.6. Запрашивать и получать от всех структурных подразделений Учреждения сведения или справочные материалы, необходимые для осуществления своей деятельности.

4.1.7. 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.

4.1.8. 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.

4.1.9. Проводить проверки соблюдения установленного порядка защиты ПДн во всех структурных подразделениях Учреждения и докладывать об их результатах директору.

4.1.10. Взаимодействовать в соответствии с законодательством РФ с федеральными органами исполнительной власти, федеральными государственными органами, органами государственной власти республики Коми, государственными органами республики Коми, органами местного самоуправления республики Коми, организациями по вопросам ИБ и защиты ПДн.

4.1.11. Вносить руководителям структурных подразделений Учреждения предложения о приостановке действий, противоречащих законодательству РФ в области ПДн, по направлениям, отнесенным к компетенции Комиссии в соответствии с разделом 3 настоящего положения.

4.1.12. Принимать необходимые меры в случае обнаружения нарушения установленного порядка защиты ПДн, вплоть до приостановки обработки ПДн в ИСПДн, структурных подразделениях или в Учреждении в целом.

4.1.13. Требовать от работников Учреждения письменных объяснений необходимых обстоятельств и фактов при проведении служебных расследований.

4.1.14. Подготавливать и представлять в установленном порядке директору предложения о порядке определения размера ущерба, который может быть причинен Учреждению, его работникам либо субъектам ПДн вследствие нарушения безопасности ПДн.

4.1.15. Вносить предложения директору об отстранении от выполнения служебных (трудовых) обязанностей работников Учреждения, систематически нарушающих требования по защите ПДн.

4.1.16. Являться инициатором применения мер дисциплинарного взыскания по отношению к работникам, нарушающим установленный порядок защиты ПДн.

4.2. Членам Комиссии запрещается:

4.2.1. Доводить до работников Учреждения сведения о СЗПДн в полном объеме.

4.2.2. При выводе из состава Комиссии раскрывать объем работ и конкретные направления деятельности Комиссии, разглашать информацию, ставшую известной в ходе работы в составе Комиссии.

5. 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	Пункт	Ответственный
Заседание Комиссии	1 раз в полгода	2.2.1	Председатель Комиссии
Контроль и оценка эффективности принимаемых мер защиты ПДн и применяемых СЗИ	Ежегодно	3.1.1.4	Комиссия
Организация и проведение учебно-методических мероприятий с работниками Учреждения по вопросам защиты ПДн	Ежеквартально	3.1.1.5	Комиссия
Контроль порядка доступа в выделенные помещения	Ежеквартально	3.2.1.1.3	Комиссия
Формирование планов резервного копирования ресурсов ИСПДн	Ежеквартально	3.2.1.1.4	Комиссия
Проведение мероприятий по очистке и (или) уничтожению машинных носителей ПДн	Ежеквартально	3.2.1.3.2	Комиссия
Анализ возможных УБПДн и каналов их утечки	Ежегодно	3.2.1.1.6	Комиссия
Контроль наличия материальных носителей ПДн	Ежеквартально	3.2.1.2.3	Комиссия
Контроль соблюдения требований технических условий, правил эксплуатации и сертификатов на эксплуатируемые СЗИ	Ежегодно	3.2.1.2.4	Комиссия

6. Ответственность

6.1. 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.

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

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

Приложение:
1. Типовая форма перечня обязанностей членов постоянно действующей комиссии по защите персональных данных на 1 л. в 1 экз.
2. Типовая форма протокола заседания постоянно действующей комиссии по защите персональных данных на 2 л. в 1 экз.

Приложение № 1
к положению о постоянно
действующей комиссии по защите
персональных данных

ТИПОВАЯ ФОРМА

перечня обязанностей членов постоянно действующей комиссии по защите персональных данных

Направление деятельности	Ф.И.О. ответственного	Подпись
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		
Резервирование и восстановление работоспособности элементов информационных систем персональных данных		
Установка, настройка и администрирование средств защиты информации, анализ системных журналов средств защиты информации		
Подготовка журналов учета системы защиты персональных данных		
Уничтожение персональных данных и их материальных носителей		