УТВЕРЖДЕН
приказом ГПОУ «УМК»
от 31.08.2016 № 42

РЕГЛАМЕНТ

проведения внутренних мероприятий по контролю обеспечения защиты персональных данных

Содержание

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Назначение

Регламент проведения внутренних мероприятий по контролю обеспечения защиты персональных данных определяет особенности проведения внутренних мероприятий по контролю обеспечения защиты персональных данных в ГПОУ «УМК».

Цели

Формализация состава и периодичности проведения контрольных мероприятий, порядка их проведения и планирования.

Формализация порядка проведения оценки соответствия обработки и защиты персональных данных в ГПОУ «УМК» требованиям законодательства РФ в области персональных данных и локальных нормативных актов ГПОУ «УМК».

Формализация порядка проведения оценки эффективности и достаточности принимаемых мер по обеспечению безопасности персональных данных в соответствии с оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения их законных прав.

Обеспечение своевременного выявления и предотвращения угроз безопасности персональных данных при их обработке в информационных системах персональных данных ГПОУ «УМК».

Область применения

Все лица, назначенные приказом директора в состав постоянно действующей комиссии по защите персональных данных, а также лица, на которых локальными нормативными актами ГПОУ «УМК» возлагается ответственность за проведение мероприятий по контролю обеспечения защиты персональных данных, в обязательном порядке должны быть ознакомлены с настоящим регламентов под подпись.

Вступление в силу

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

Все изменения вносятся приказом директора. Полный плановый пересмотр осуществляется регулярно, не реже одного раза в год, с целью проверки соответствия положений реальным условиям обработки и защиты персональных данных в ГПОУ «УМК». Частичный пересмотр осуществляется по мере необходимости постоянно действующей комиссией по защите персональных данных в следующих случаях:

- при изменении приоритетов угроз безопасности персональных данных;
- при изменении процессов обработки персональных данных, местонахождения объектов защиты, условий их содержания, хранения и использования;
- при определении такой необходимости по результатам проведения внутреннего контроля обеспечения защиты персональных данных, в целях повышения эффективности мероприятий, определенных в настоящем регламенте;

– при изменении состава, обязанностей и полномочий должностных лиц ГПОУ «УМК», задействованных в вводимых настоящим регламентом мероприятиях.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аудит информационной безопасности (организации) – систематический, независимый и документированный процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации (ГОСТ Р 53114-2008).

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

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).

Контроль обеспечения защиты персональных данных – проверка соответствия обеспечения защиты персональных данных в организации, наличия и содержания документов требованиям нормативных документов, технической, правовой, организационно-распорядительной документации в области защиты персональных данных.

Критерий аудита информационной безопасности (организации) – совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности (ГОСТ Р 53114-2008).

Матрица доступа – таблица, отображающая правила разграничения доступа («Защита от несанкционированного доступа к информации. Термины и определения», утверждено решением председателя Гостехкомиссии России от 30.03.1992)

Мониторинг информационной безопасности (организации) – постоянное наблюдение за процессом обеспечения информационной безопасности в организации с целью установить его соответствие требованиям по информационной безопасности (ГОСТ Р 53114-2008).

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).

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).

Обеспечение информационной безопасности (организации) – деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз (ГОСТ Р 53114-2008).

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).

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

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 50922-2006).

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).

Оценка соответствия требованиям по защите информации – прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации (ГОСТ Р 50922-2006).

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).

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа («Защита от несанкционированного доступа к информации. Термины и определения», утверждено решением председателя Гостехкомиссии России от 30.03.1992).

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).

Цель защиты информации – заранее намеченный результат защиты информации (ГОСТ Р 50922-2006).

Примечание: результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию, или обеспечение соответствия требованиям в области защиты информации.

Эффективность защиты информации – степень соответствия результатов защиты информации цели защиты информации (ГОСТ Р 50922-2006).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Годовой план	– годовой план мероприятий по обеспечению безопасности персональных данных;
Журнал	– Журнал учета мероприятий по контролю обеспечения безопасности персональных данных;
ИБ	– информационная безопасность;
ИСПДн	– информационная система персональных данных;
Контроль	– контроль обеспечения защиты персональных данных;
ЛНА	– локальные нормативные акты;
МНИ	– машинный носитель информации;
НСД	– несанкционированный доступ;
ПДн	– персональные данные;
ПО	– программное обеспечение;
СЗИ	– средство защиты информации;
СЗПДн	– система защиты персональных данных;
УБПДн	– угрозы безопасности персональных данных;
Учреждение	– ГПОУ «УМК».

1. Общие положения

1.1. Контроль в Учреждении осуществляется с целью своевременного выявления и предотвращения НСД к ПДн и других УБПДн, актуальных для ИСПДн, определенных по нормам и методикам, утвержденным ФСТЭК России.

1.2. Контроль и оценка эффективности защиты ПДн являются неотъемлемой составной частью работ по защите ПДн при создании и эксплуатации ИСПДн.

1.3. Основными задачами Контроля являются:

- проверка соответствия принятых и принимаемых мер по защите ПДн требованиям законодательства РФ и ЛНА Учреждения;
- проверка своевременности и полноты выполнения требований нормативных документов, регламентирующих организацию и порядок осуществления мероприятий по защите ПДн.

1.4. Результат проведения контрольных мероприятий служит подтверждение того, что:

- СЗПДн обеспечивает выполнение требований законодательства РФ в области защиты ПДн при эксплуатации ИСПДн;
- меры, средства и мероприятия, проводимые в целях защиты ПДн, обеспечивают необходимый уровень защищенности ПДн при их обработке в ИСПДн;
- СЗИ настроены и используются в соответствии с техническими условиями, правилами эксплуатации и требованиями формуляров;
- рекомендации предшествующих проверок реализованы в полной мере.

1.5. Постоянный внутренний Контроль осуществляется Комиссией в рамках исполнения ею своих обязанностей.

1.6. Результаты Контроля оформляются актами, протоколами, заключениями и записями в специальных журналах и доводятся до сведения директора и должностных лиц в соответствии с уровнем Контроля.

1.7. Полная внутренняя проверка условий обработки и защиты ПДн проводится Комиссией не реже 1 раза в 3 года в сроки, определяемые Комиссией, и санкционируется приказом директора.

1.8. По инициативе Учреждения может проводиться аудит обеспечения безопасности ПДн с привлечением третьей стороны – юридических лиц или индивидуальных предпринимателей, имеющих лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, заключающийся в оценке соответствия текущего состояния ИБ в Учреждении требованиям правовых и нормативных документов в области защиты ПДн.

2. Организация Контроля

2.1. Виды Контроля

2.1.1. Комиссия проводит как плановый (периодический), так и внеплановый Контроль. Время проведения внепланового Контроля проверяемым не сообщается. Порядок проведения Контроля определяется ЛНА Учреждения, включая настоящий регламент, и соответствующими методиками.

2.1.2. Повседневный (оперативный) Контроль над выполнением требований по защите ПДн осуществляют лица, ответственные за эксплуатацию ИСПДн, обработку ПДн, а также члены Комиссии и другие уполномоченные приказами директора лица.

2.2. Состав контрольных мероприятий

2.2.1. Основными составляющими Контроля являются:

2.2.1.1. Автоматизированный контроль на основе мониторинга событий ИБ.

2.2.1.2. Проверка правильности и полноты проводимых мероприятий по обеспечению соответствия обработки и защиты ПДн требованиям законодательства РФ.

2.2.1.3. Проверка работоспособности и эффективности СЗИ. Проверка работоспособности СЗИ в рамках контрольных мероприятий проводится в соответствии с программой проведения контроля состояния СЗПДн.

2.2.1.4. Проверка своевременности внесения изменений в проектную, техническую и нормативно-техническую документацию по обеспечению безопасности ПДн.

2.2.1.5. Принятие на основе результатов Контроля мер по устранению последствий нарушений требований безопасности ПДн, вплоть до полного или частичного приостановления эксплуатации ИСПДн, если иными мерами невозможно устранить нарушения требований безопасности ПДн.

2.2.1.6. Проведение в ходе мероприятий по государственному контролю разъяснительной работы по применению требований законодательства РФ и нормативных документов в области защиты ПДн в ИСПДн.

2.2.2. Основные контрольные мероприятия и периодичность их проведения приведены в таблице 1.

Таблица 1 – Перечень основных контрольных мероприятий

Мероприятие	Периодичность
Контроль соответствия полномочий пользователей ИСПДн матрицам доступа	Ежемесячно
Контроль соблюдения порядка и требований обработки ПДн	Еженедельно
Контроль соблюдения требований парольной защиты	Ежемесячно
Контроль соблюдения требований антивирусной защиты	Еженедельно
Контроль соблюдения требований ИБ в сфере информационного обмена	Еженедельно
Контроль соблюдения требований работы с МНИ	Ежемесячно

Контроль соблюдения порядка доступа в выделенные помещения	Ежеквартально
Контроль соблюдения порядка проведения резервного копирования, хранения и корректности создаваемых резервных копий	Ежемесячно
Контроль соблюдения порядка использования СЗИ	Еженедельно
Контроль соблюдения требований хранения материальных носителей ПДн (бумажных и машинных)	Ежеквартально
Контроль соблюдения требований работы в ИСПДн	Ежемесячно
Контроль соответствия состава обрабатываемых ПДн заявленным целям их обработки	Ежегодно
Контроль реагирования на обращения (запросы) субъектов ПДн об исполнении из законных прав	Ежемесячно
Контроль исполнения требований Комиссии	Ежеквартально
Контроль (тестирование) работоспособности и корректной настройки СЗПДн	Ежеквартально
Контроль удаления ПДн и уничтожения их материальных носителей	Ежеквартально
Контроль соблюдения порядка предоставления ПДн и их материальных носителей третьим лицам	Ежемесячно
Выявление изменений порядка и условий обработки и защиты ПДн	Ежегодно
Контроль обновления ПО и соответствия программного и технического состава ИСПДн заявленному (техническому паспорту)	Ежемесячно
Анализ и переоценка УБПДн, предсказание появления новых, еще не известных угроз	Ежегодно
Контроль исполнения требований законодательства РФ в области ПДн	Ежеквартально
Контроль актуальности ЛНА, регламентирующих обработку и защиту ПДн	Ежеквартально
Контроль ведения журнальных форм	Ежеквартально
Внутренний аудит обеспечения безопасности ПДн	1 раз в 3 года

2.2.3. Периодичность проведения того или иного мероприятия устанавливается по решению Комиссии. Некоторые мероприятия следует проводить внепланово, в случае изменения внешних факторов, например, изменения законодательства РФ в области ПДн.

2.3. Планирование

2.3.1. Внутренние мероприятия по Контролю могут быть:

- плановыми;
- внеплановыми.

2.3.2. Плановые мероприятия

2.3.2.1. Плановые мероприятия устанавливаются ЛНА Учреждения, регламентирующими обработку и защиту ПДн, включая настоящий регламент.

2.3.2.2. Перечень плановых мероприятий формируется Комиссией и утверждается директором в виде годового плана.

2.3.3. Внеплановые мероприятия

2.3.3.1. Решение о проведении внеплановых мероприятий принимается председателем Комиссии, и оформляется приказом директора.

2.3.3.2. Внеплановость мероприятий подразумевает:

- максимально короткий срок между выходом приказа о проведении и проведением;
- минимизация круга лиц, которые заранее знают о готовящемся мероприятии;
- отсутствие периодичности в сроках проведения таких мероприятий.

2.3.3.3. Внеплановые мероприятия могут осуществляться, в частности, в следующих случаях:

- при изменении законодательства РФ в области ПДн;
- при возникновении или после возникновения инцидента ИБ (например, утечки ПДн);
- появления жалоб субъектов ПДн;
- изменения структуры процессов обработки ПДн.

2.3.3.4. Внеплановые мероприятия могут осуществляться, в частности, в целях:

- реагирования на инциденты ИБ и их предупреждения;
- определения текущего состояния СЗПДн;
- определения уровня подготовки работников в области защиты ПДн;
- тестирования СЗПДн.

2.3.3.5. В качестве внеплановых мероприятий могут выступать любые мероприятия из входящих в состав плановых, а также иные.

3. Проведение Контроля

3.1. Внутренний плановый Контроль проводится Комиссией в соответствии с годовыми планами. Планы, как правило, составляются на один календарный год таким образом, чтобы в течение года была проведена проверка выполнения всех требований к обеспечению безопасности ПДн и условиям их обработки.

3.2. При проведении внутреннего планового Контроля Комиссия:

- проверяет наличие необходимых ЛНА и эксплуатационных документов на СЗИ и знание их работниками Учреждения;
- проверяет выполнение требований ЛНА Учреждения и эксплуатационных документов на СЗИ работниками Учреждения;
- документирует результаты Контроля;
- вырабатывает рекомендации по устранению недостатков в обеспечении ИБ и по совершенствованию СЗПДн.

3.3. Результаты проведения внутренних мероприятий по контролю фиксируются в протоколах проведения внутренних проверок. В случае выявления нарушения, председателем Комиссии в протоколе делается запись о мероприятиях по устранению нарушения и сроке исполнения. Протоколы хранятся у председателя Комиссии до конца текущего года. Уничтожение протоколов проводится Комиссией самостоятельно в январе следующего за проверочным годом.

3.4. По результатам внутреннего планового Контроля разрабатывается план по устранению недостатков в обеспечении ИБ и совершенствованию СЗПДн, в соответствии с которым в Учреждении разрабатываются и проводятся необходимые мероприятия.

3.5. О результатах внутреннего Контроля и мерах, необходимых для устранения нарушений, директору докладывает председатель Комиссии.

3.6. При повседневном Контроле осуществляется анализ событий, произошедших в ИСПДн, по различным системным журналам, включая журналы СЗИ от НСД. Для расследования инцидентов, связанных с нештатными ситуациями или нарушением безопасности ПДн, в Учреждении могут создаваться специальные комиссии.

3.7. Все проводимые мероприятия по защите ПДн подлежат обязательному учету в Журнале.

3.8. Сведения о проведенном мероприятии заносится в Журнал проводившим мероприятие лицом сразу после осуществления данного мероприятия.

3.9. В случае невозможности проведения того или иного мероприятия в запланированный заранее день, оно может быть проведено ранее или позднее (не более чем на неделю) намеченной даты.

4. Годовой план мероприятий

4.1. Общие сведения

4.1.1. Комиссией ежегодно формируется Годовой план на один (следующий) год для каждого из ответственных лиц. После формирования годовые планы утверждаются директором.

4.1.2. Годовой план на следующий год должен быть подготовлен и утвержден не позднее 15 декабря текущего года.

4.1.3. После утверждения годовой план передается ответственному лицу. В случае, если в качестве ответственного лица выступает Комиссия, план передается ее председателю.

4.1.4. Вопросы пересмотра плана на текущий год решаются на заседании Комиссии.

4.1.5. Выполненные планы передаются ответственному лицу и хранятся в течение трех лет.

4.2. Структура годового плана

4.2.1. В годовой план включаются все устанавливаемые ЛНА Учреждения мероприятия в области защиты ПДн, мероприятия для данного ответственного с указанием их наименований и дат проведения. В целях упрощения определения состава мероприятий, вводимых тем или иным ЛНА Учреждения, каждый такой акт (в том числе и настоящий регламент) может содержать раздел «Сводный перечень регулярных мероприятий».

4.2.2. Годовой план состоит из двух разделов:

- еженедельные мероприятия (и более частые);
- прочие мероприятия.

4.2.3. В первый раздел годового плана включаются мероприятия, выполнение которых необходимо осуществлять еженедельно или чаще (ежедневно, два раза в неделю и т.п.). Данную часть плана рекомендуется оформлять в виде таблицы из 7-ми строк – на каждый день недели. В каждой ячейке этой таблицы необходимо указать соответствующие мероприятия и ссылку на ЛНА Учреждения, их вводящий.

4.2.4. Во второй раздел включаются мероприятия, осуществляемые с периодичностью от одного раза в неделю (не включительно). Каждое такое мероприятие должно быть привязано к конкретной дате, в которую данное мероприятие должно быть проведено. При выборе даты проведения мероприятия необходимо ориентироваться по календарю выходных и праздничных дней на соответствующий год. В целях повышения удобства использования годового плана, мероприятия в данном разделе группируются сначала по месяцам, потом – по датам. Причем, даты должны располагаются в порядке от 1 января до 31 декабря.

4.3. Обновление годового плана

4.3.1. Вопросы обновления годового плана на текущий год рассматриваются на заседаниях Комиссии.

4.3.2. При необходимости дополнить годовой план новыми мероприятиями, либо изменить состав или порядок мероприятий в плане на оставшийся период года – годовой план изменяется.

4.3.3. Мероприятия, размещенные в старой версии плана, в новую не переносятся. Новая версия должна содержать только мероприятия, актуальные до конца года. На обложке новой версии плана указывается с какой даты он действует.

4.3.4. Обновленная версия утверждается директором и незамедлительно, в течение одного дня, передается ответственному лицу, старая версия изымается. На обложке старой версии годового плана делается пометка о его неактуальности, начиная с указанной даты.

4.4. Обращение ответственного с годовым планом

4.4.1. Ответственный за выполнение мероприятий годового плана обязан ежедневно уточнять состав ближайших мероприятий с целью подготовки к ним, а также выполнять все мероприятия, запланированные на текущий день.

4.4.2. Ответственный обязан обеспечить сохранность находящегося у него годового плана и предоставлять его по требованию Комиссии (но не более чем на один день).

4.4.3. По окончании года ответственный обязан передать план председателю Комиссии.

4.5. Контроль выполнения плановых мероприятий

4.5.1. Контроль выполнения плановых мероприятий осуществляется ежеквартально Комиссией.

4.5.2. Для контроля Комиссией привлекается соответствующий годовой план (в том числе его старые версии, при необходимости) и Журнал.

4.5.3. Осуществляется контроль выполнения мероприятий за истекший квартал.

4.5.4. В случае невыполнения без уважительных причин запланированных мероприятий, ответственное лицо может быть подвергнуто дисциплинарному взысканию.

5. Сводный перечень регулярных мероприятий

5.1. Сводный перечень регулярных мероприятий, вводимых настоящим регламентом, представлен в таблице 2, в которой для каждого мероприятия указаны:

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

Таблица 2 – Сводный перечень регулярных мероприятий

Наименование мероприятия	Периодичность	Пункт	Ответственный
Контрольные мероприятия	в соответствии с таблицей 1	2.2.2	Комиссия
Формирование годового плана	ежегодно, до 15 декабря	4.1.2	Комиссия
Контроль выполнения плановых мероприятий по обеспечению защиты ПДн	ежеквартально	4.5.1	Комиссия

6. Ответственность

6.1. Лица, ответственные за проведение мероприятий по Контролю, несут персональную ответственность за качество и своевременность проведения возложенных на них мероприятий в соответствии с настоящим регламентом и действующим законодательством РФ.

Приложение:

1. Типовая форма протокола проведения внутренней проверки условий обработки и защиты персональных данных на 2 л. в 1 экз.
2. Типовая форма годового плана мероприятий по обеспечению безопасности персональных данных постоянно действующей комиссией по защите персональных данных на 4 л. в 1 экз.
3. Алгоритм проведения полной внутренней проверки условий обработки и защиты персональных данных и приложение к нему, всего на 8 л. в 1 экз.

Приложение № 1
к Регламенту проведения внутренних мероприятий по контролю обеспечения защиты персональных данных

ТИПОВАЯ ФОРМА

Государственное профессиональное
образовательное учреждение
«Ухтинский медицинский колледж»
(ГПОУ «УМК»)

ПРОТОКОЛ

_____ № _____

г. Ухта

проведения внутренней проверки условий
обработки и защиты персональных данных

Настоящий протокол составлен в том, что ___.___.201__ постоянно действующей комиссией по защите персональных данных, в составе:

Председатель комиссии – Зименко Борис Сергеевич (заместитель директора по ЭВ);
Члены комиссии – Саркиц Владислав Михайлович (техник-программист);
– Бляндур Мария Ивановна (главный бухгалтер).

проведена внутренняя проверка: _____
_____.
(тема проверки)

Внутренняя проверка осуществлялась в соответствии с требованиями:
_____.
(название документа)

В ходе внутренней проверки проверено:
_____
_____.
(состав проведенных мероприятий)

Выявленные нарушения:
_____
_____.

Меры по устранению нарушений:
_____
_____.

Срок устранения нарушений: _____.

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

(должность руководителя проверяемого подразделения)

Приложение № 2
к Регламенту проведения внутренних мероприятий по контролю обеспечения защиты персональных данных

ТИПОВАЯ ФОРМА

ГОДОВОЙ ПЛАН

мероприятий по обеспечению безопасности персональных данных
постоянно действующей комиссией по защите персональных данных

на 201__ год

ЕЖЕНЕДЕЛЬНЫЕ мероприятия

День недели	Наименование мероприятия	Ответственный	Примечание
Понедельник			
Вторник			
Среда			
Четверг			
Пятница			

Мероприятия на ЯНВАРЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на ФЕВРАЛЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на МАРТ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на АПРЕЛЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на МАЙ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на ИЮНЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на ИЮЛЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на АВГУСТ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на СЕНТЯБРЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на ОКТЯБРЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на НОЯБРЬ

Дата проведения	Наименование мероприятия	Основание	Примечание

Мероприятия на ДЕКАБРЬ

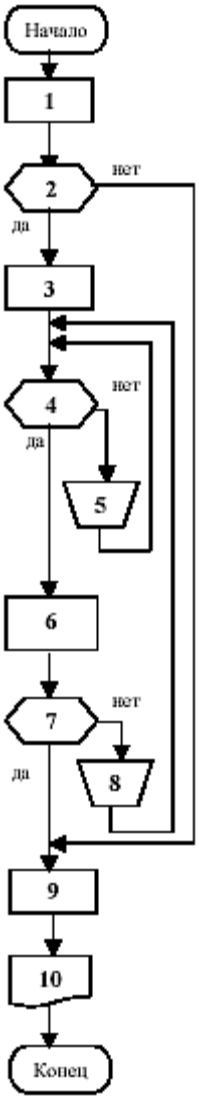
Дата проведения	Наименование мероприятия	Основание	Примечание

Приложение № 3
к Регламенту проведения внутренних мероприятий по контролю обеспечения защиты персональных данных

АЛГОРИТМ

проведения полной внутренней проверки условий обработки и защиты персональных данных

Полная внутренняя проверка условий обработки и защиты персональных данных проводится поэтапно:



0. Началом работы является приказ директора о проведении полной внутренней проверки условий обработки и защиты персональных данных.
1. Анализ выявленных нарушений, установление причин.
2. Оценка необходимости разработки мер по устранению нарушений.
3. Разработка мер по устранению нарушений.
4. Согласование и утверждение мер по устранению нарушений.
5. Доработка мер по устранению нарушений.
6. Внедрение мер по устранению нарушений.
7. Проверка эффективности мер по устранению нарушений.
8. Разработка дополнительных пер по устранению нарушений.
9. Утверждение протокола анализа нарушений, выявленных в ходе проведения полной внутренней проверки условий обработки и защиты персональных данных.
10. Протокол анализа нарушений, выявленных в ходе проведения полной внутренней проверки условий обработки и защиты персональных данных.

Приложение:

1. Типовая форма акта проведения полной внутренней проверки условий обработки и защиты персональных данных на 2 л. в 1 экз.
2. Типовая форма протокола проведения полной внутренней проверки условий обработки и защиты персональных данных на 3 л. в 1 экз.
3. Типовая форма протокола анализа нарушений, выявленных в ходе проведения полной внутренней проверки условий обработки и защиты персональных данных на 2 л. в 1экз.

Приложение № 1
к приложению № 3

ТИПОВАЯ ФОРМА

Государственное профессиональное
образовательное учреждение
«Ухтинский медицинский колледж»
(ГПОУ «УМК»)

УТВЕРЖДАЮ
Директор
ГПОУ «УМК»
_____ А.В. Данильченко
___.___.201__

АКТ

_____ № _____

г. Ухта

проведения полной внутренней проверки
условий обработки и защиты персональных данных

Основание: приказ директора от ___.___.201_ № _____ «О проведении полной внутренней проверки условий обработки и защиты персональных данных».

Составлен комиссией, в составе:

Председатель комиссии – Зименко Борис Сергеевич (заместитель директора по ЭВ);
Члены комиссии – Саркиц Владислав Михайлович (техник-программист);
– Бляндур Мария Ивановна (главный бухгалтер).

Комиссия ___.___.201_ провела полную внутреннюю проверку условий обработки и защиты персональных данных в ГПОУ «УМК», по адресу: Республика Коми, г. Ухта, ул. Чибьюская, 28.

Проверка осуществлялась в соответствии с:

- требованиями законодательства РФ в области персональных данных;
- требованиями локальных нормативных актов.

В ходе проверки проверено:

- локальная нормативная база;
- организация системы защиты персональных данных;
- реализация технической защиты информации;
- обучение и ознакомление работников;
- регулярность проведения периодических проверочных мероприятий.

В ходе проверки:

1. Установлены следующие оценки: 0 баллов _____;
   1 балл _____;
   2 балла _____;
   3 балла _____.

Итоговая оценка: _____.

Протокол проведения полной внутренней проверки условий обработки и защиты персональных данных прилагается.

2. Выявлены нарушения, подлежащие устранению:

– _____;
– _____;
– _____;
– _____;
– _____;
– _____.

По итогам проверки проведен анализ нарушений и разработаны меры по их устранению:

– _____;
– _____;
– _____;
– _____;
– _____;
– _____.

Протокол анализа нарушений, выявленных в ходе проведения полной внутренней проверки условий обработки и защиты персональных данных прилагается.

Меры по устранению нарушений полностью/(частично) выполнены, проверка эффективности проведена, повторная проверка проведена. Все нарушения устранены/(Нарушения не устранены, требуются дополнительные меры по их устранению).

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____

_____ _____

Приложение № 2
к приложению № 3

ТИПОВАЯ ФОРМА

Государственное профессиональное
образовательное учреждение
«Ухтинский медицинский колледж»
(ГПОУ «УМК»)

ПРОТОКОЛ

_____ № _____

г. Ухта

проведения полной внутренней проверки
условий обработки и защиты персональных данных

Настоящий протокол составлен в том, что ___.___.201__ постоянно действующей комиссией по защите персональных данных, в составе:

Председатель комиссии – Зименко Борис Сергеевич (заместитель директора по ЭВ);
Члены комиссии – Саркиц Владислав Михайлович (техник-программист);
– Бляндур Мария Ивановна (главный бухгалтер).

проведена полная внутренняя проверка условий обработки и защиты персональных данных в ГПОУ «УМК» (далее – Учреждение), по адресу: Республика Коми, г. Ухта, ул. Чибьюская, 28.

В ходе проверки оценивалась локальная нормативная база, организация системы защиты персональных данных, реализация технической защиты информации, обучение и ознакомление работников и регулярность проведения плановых контрольных мероприятий.

Оценки выставлялись следующим образом:

- критерий полностью соответствует действующим нормам и выполняется – 3 балла;
- критерий полностью соответствует действующим нормам, но не выполняется – 2 балла;
- критерий не полностью соответствует действующим нормам, но выполняется – 2 балла;
- критерий не полностью соответствует действующим нормам и не выполняется – 1 балл;
- критерий не соответствует действующим нормам, но выполняется – 1 балл;
- критерий не соответствует действующим нормам и не выполняется – 0 баллов.

Результаты оценки содержатся в таблице ниже.

Таблица – Оценки

№	Критерий	Оценка				Примечание
		3	2	1	0	
Локальная нормативная база						
1.	Полнота организационно-распорядительной документации по обеспечению системы защиты персональных данных					
2.	Актуальность перечня обрабатываемых персональных данных					
3.	Полнота содержащихся сведений в типовых формах					
4.	Актуальность документации об организации системы защиты персональных данных					
5.	Актуальность технической документации об организации системы защиты персональных данных					
6.	Наличие введенных журнальных форм по различным видам учета					
Организация системы защиты персональных данных						
7.	Назначение ответственного за обеспечение системы защиты персональных данных					
8.	Организация порядка допуска в выделенные помещения					
9.	Организация разграничения прав доступа к информационным системам персональных данных					
10.	Организация архивного хранения документов, содержащих персональные данные					
11.	Публикация политики Учреждения в отношении обработки персональных данных в общедоступном месте					
12.	Назначение ответственного за регистрацию запросов от субъектов персональных данных					
13.	Назначение ответственных за ведение журнальных форм					
14.	Организация учета средств защиты информации, криптографических средств					
15.	Организация учета машинных носителей информации					
16.	Организация учета входящих и исходящих документов, содержащих персональные данные					
Техническая защита информации						
17.	Исполнение требований по реализации антивирусной защиты					
18.	Исполнение требований по реализации разграничения прав доступа					
19.	Исполнение требований по реализации резервного копирования					

№	Критерий	Оценка				Примечание
		3	2	1	0	
20.	Исполнение требований по реализации межсетевого экранирования					
21.	Исполнение требований по реализации защиты от несанкционированного доступа					
22.	Исполнение требований по реализации контроля машинных носителей информации					
23.	Контроль установленного ПО, не связанного с должностными обязанностями					
Обучение и ознакомление персонала						
24.	Проведения обучения работников на предмет знания основ работы с персональными данными					
25.	Ознакомление работников с действующей документацией об организации системы защиты персональных данных					
26.	Ознакомление работников с инструкциями о порядке работы с персональными данными					
27.	Обучение руководителей структурных подразделений о порядке обработки персональных данных в структурном подразделении в соответствии с функциями и задачами					
Исполнение обязательных проверочных мероприятий						
28.	Проведение регулярных проверок в соответствии с планом мероприятий					
29.	Осуществление проверок знаний о порядке организации обработки и защиты персональных данных					
Итого: количество ответов по столбцам						
Количество баллов по столбцам						
Фактическое кол-во баллов / / Возможное кол-во баллов						Итоговая оценка:

Председатель комиссии _____ _____

Члены комиссии _____ _____

_____ _____

_____ _____

Приложение № 3
к приложению № 3

ТИПОВАЯ ФОРМА

Государственное профессиональное
образовательное учреждение
«Ухтинский медицинский колледж»
(ГПОУ «УМК»)

ПРОТОКОЛ

_____ № _____

г. Ухта

анализа нарушений, выявленных в ходе проведения
полной внутренней проверки условий обработки
и защиты персональных данных

1. Исходные данные: протокол проведения полной внутренней проверки условий обработки и защиты персональных данных от ___.___.201__ № _______.

Описание выявленных нарушений:

1.1. _____.
1.2. _____.
1.3. _____.
1.4. _____.
1.5. _____.
1.6. _____.

Результаты анализа существования (актуальности) нарушений:

1.1. _____.
1.2. _____.
1.3. _____.
1.4. _____.
1.5. _____.
1.6. _____.

2. Меры по устранению нарушений целесообразны:

_____ _____ _____
(да/нет) подпись инициалы, фамилия

3. Меры по устранению нарушений «Утверждаю»: _____ _____
подпись инициалы, фамилия

№	Содержание мер по устранению нарушений	Ответственный	Срок	Отметка о выполнении

1.				
2.				
3.				
4.				
5.				
6.				

4. _____ провести проверку эффективности в срок до ___.___.201__.
(ответственному)

_____.
(способ и (или) метод проверки)

5. Проверка эффективности проведена: Дата _____ Результат _____
_____.

6. Необходимы дополнительные меры по устранению нарушений:

_____ _____ _____
(да/нет) подпись инициалы, фамилия

– _____;
– _____;
– _____;
– _____;
– _____;

Меры по устранению нарушений согласованы и составлены.

Председатель комиссии _____ _____

Члены комиссии _____ _____
_____ _____
_____ _____