Приложение № 2
К приказу РАМ имени Гнесиных
От «24» 07 2020 № 783а

П О Л О Ж Е Н И Е

О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В РАМ ИМЕНИ ГНЕСИНЫХ

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Доступ к информации — возможность получения информации и ее использования.

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 способ осуществления таких процессов и методов.

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.

Контролируемая зона — пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание сторонних лиц, а также транспортных, технических и иных материальных средств.

Несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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.

Оператор — 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.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки — электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное (программно-математическое) воздействие — несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технический канал утечки информации — совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных — совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам — неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо — лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации — способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Таблица 1. Условные обозначения и сокращения

Сокращение	*Значение*
АС	Автоматизированная система
ИСПДн	Информационная система персональных данных
ЛВС	Локальная вычислительная сеть
ОРД	Организационно-распорядительная документация
ПДн	Персональные данные
НСД	Несанкционированный доступ
ПДТК	Постоянно действующая техническая комиссия
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
СВТ	Средство вычислительной техники
СЗПДн	Система защиты персональных данных
СТР-К	Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации» (утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282)
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение о порядке организации и проведения работ по защите персональных данных (далее — Положение) в Федеральном государственном бюджетном образовательном учреждении высшего образования «Российская академия музыки имени Гнесиных» Министерства культуры Российской Федерации (далее – РАМ имени Гнесиных) разработано во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и определяет содержание и порядок осуществления мероприятий по защите ПДн, обрабатываемых с использованием средств автоматизации, в РАМ имени Гнесиных.

1.1 Цель Положения

Целью данного Положения является регламентация организации и проведения работ по защите ПДн и приведение существующих информационных систем в надлежащий вид в соответствии с действующими требованиями по безопасности ПДн.

Мероприятия по защите ПДн с грифом «Конфиденциально» являются неотъемлемой составной частью деятельности в РАМ имени Гнесиных.

Уровень технической защиты ПДн, а также перечень необходимых мер защиты определяются дифференцированно по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты ПДн и величины ущерба, который может быть нанесен субъектам ПДн.

1.2 Объекты защиты

В РАМ имени Гнесиных подлежат защите АС, ЛВС, средства и системы связи и передачи информации, другие технические средства, используемые для обработки ПДн.

Защита ПДн в РАМ имени Гнесиных обеспечивается выполнением комплекса организационных мероприятий и применением средств защиты ПДн от утечки по техническим каналам, НСД, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности ПДн в процессе их обработки, передачи и хранения, а также обеспечения работоспособности технических средств.

1.3 Ответственные за защиту

Организация защиты ПДн на объекте информатизации возлагается на ответственного за организацию работ по защите ПДн, назначаемого приказом ректора РАМ имени Гнесиных.

Должностные лица, в обязанность которых входит обработка ПДн, обязаны обеспечить каждому субъекту ПДн возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Настоящее Положение является обязательным для исполнения всеми работниками, ответственными за защиту ПДн.

2 НОРМАТИВНО-МЕТОДИЧЕСКАЯ ДОКУМЕНТАЦИЯ

При организации и проведении работ по защите ПДн необходимо руководствоваться следующими нормативными и методическими документами:

– Конституция Российской Федерации;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Указ Президента от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

– Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119);

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.);

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 14 февраля 2008 г.);

– Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622);

– Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/5-144);

– Специальные требования и рекомендации по технической защите конфиденциальной информации (утв. приказом Гостехкомиссии России от 30 августа 2002 г. № 282);

– Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (зарегистрировано в Минюсте России 18 августа 2014 г. № 33620);

– Информационное сообщение ФСТЭК России от 6 марта 2015 г. № 240/22/879 «О банке данных угроз безопасности информации»;

– Приказ ФСТЭК России от 15 февраля 2017 г. № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17».

– Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

3 ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ПДн ПРИ ИХ ОБРАБОТКЕ В ИСПДн

3.1 Организационные мероприятия

Организационные меры по защите ПДн в РАМ имени Гнесиных включают в себя следующие мероприятия:

– определение лиц (подразделений), ответственных за защиту ПДн;

– определение перечня обрабатываемых ПДн;

– определение цели обработки ПДн;

– определение сроков обработки и хранения ПДн;

– определение круга лиц, допущенных к обработке ПДн;

– организация доступа в помещения, где осуществляется обработка ПДн;

– обучение работников, допущенных к обработке ПДн, основам информационной безопасности;

– учет применяемых технических средств защиты ПДн;

– учет носителей ПДн;

– разработка ОРД.

3.2 Определение лиц (подразделений), ответственных за защиту персональных данных в РАМ имени Гнесиных

Для определения лиц (подразделений), ответственных за защиту ПДн, необходимо:

1) разработать и утвердить Положение о работнике (структурном подразделении), отвечающем за защиту ПДн;

2) разработать и утвердить должностные инструкции (либо внести изменения в существующие должностные инструкции) работников, отвечающих за защиту ПДн;

3) определить состав и утвердить ПДТК по защите информации в РАМ имени Гнесиных.

3.3 Определение перечня персональных данных, обрабатываемых в РАМ имени Гнесиных

В рамках настоящего Положения к защищаемой информации (ПДн) относится документированная конфиденциальная информация, обрабатываемая в РАМ имени Гнесиных, созданная в РАМ имени Гнесиных или полученная от юридических или физических лиц на законных основаниях.

В первую очередь, необходимо установить перечень ПДн, которые обрабатываются в РАМ имени Гнесиных.

Конфиденциальность массивов документов, создаваемых в ЛВС РАМ имени Гнесиных (библиотеках, архивах, банках данных), определяется ПДТК РАМ имени Гнесиных. Состав ПДТК РАМ имени Гнесиных определяется приказом ректора РАМ имени Гнесиных.

Конфиденциальность массивов документов, массивов документов в информационных системах (библиотеках, архивах, фондах, банках данных), создаваемых вне РАМ имени Гнесиных, определяется органами государственной власти, в ведении которых они находятся, либо непосредственно их обладателем.

3.4 Определение цели обработки персональных данных

3.4.1 Цели обработки ПДн:

– выполнение обязательств работодателя по трудовому договору;

– выполнение обязательств по предоставлению образовательных услуг студентам;

– обеспечение физического контроля доступа.

3.4.2 Определение сроков обработки и хранения ПДн

Сроки хранения и обработки информации, содержащей ПДн субъектов, определяются в соответствии с Перечнем типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения (утв. решением Росархива от 6 октября 2000 г.); в соответствии с Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (п. 4, ст. 7); и указываются в утвержденном ректором РАМ имени Гнесиных Перечне персональных данных, обрабатываемых в РАМ имени Гнесиных.

По достижении срока хранения и обработки информации, содержащей ПДн субъектов, данная информация должна быть уничтожена.

Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются.

3.4.3 Определение круга лиц, допущенных к обработке ПДн

Круг лиц, допущенных к обработке ПДн, определяется каждым руководителем подразделения, в котором обрабатываются ПДн, и утверждается ректором РАМ имени Гнесиных.

Все лица, допущенные к обработке ПДн, должны быть ознакомлены с организационно-распорядительной документацией по защите ПДн в РАМ имени Гнесиных.

В должностные инструкции работников, принимающих участие в обработке ПДн, должны быть внесены изменения в части защиты ПДн.

3.4.4 Организация доступа в помещения, где осуществляется обработка ПДн

Приказом ректора РАМ имени Гнесиных утверждается перечень лиц, допущенных в помещение (серверную), где располагаются сервера и телекоммуникационное оборудование.

В целях обеспечения ограниченного доступа в серверную входная дверь должна быть снабжена функцией автоматической системы контроля доступа. В случае, если установка данной системы невозможна, необходимо регистрировать вход/выход работников в соответствии с Перечнем лиц, допущенных в серверное помещение.

Должна осуществляться физическая охрана помещений информационных систем персональных данных (далее — ИСПДн). В качестве физической охраны помещений может использоваться централизованная система видеонаблюдения.

Доступ в помещения, где обрабатываются ПДн, лицам, не допущенным к обработке ПДн, должен быть запрещен. В случае невозможности запретить доступ в помещения, необходимо исключить возможность НСД к техническим средствам обработки ПДн, хищение и нарушение работоспособности, хищение носителей информации.

3.4.5 Обучение работников

Не реже одного раза в год сотруднику, ответственному за защиту ПДн, необходимо проводить обучение лиц, использующих средства защиты информации, применяемые в ИСПДн, правилам работы с ними. Также проводится обучение работников РАМ имени Гнесиных, допущенных к обработке ПДн, правилам обработки ПДн, в соответствии с утвержденными требованиями.

Сотруднику, проводившему обучение, необходимо заносить все мероприятия по обучению в Журнал инструктажа пользователей ИСПДн и обслуживающего персонала РАМ

имени Гнесиных по правилам обработки ПДн и в Журнал учета мероприятий по защите информации в РАМ имени Гнесиных.

3.4.6 Учет применяемых технических средств защиты ПДн

Учет технических средств защиты ПДн ведется в Техническом паспорте ИСПДн в соответствии с требованиями СТР-К.

3.4.7 Технические мероприятия

Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов РАМ имени Гнесиных.

3.4.8 Требования к техническим и программным средствам

Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

3.4.9 Необходимость создания СЗПДн

Создание СЗПДн является необходимым условием обеспечения безопасности ПДн в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиями к обеспечению безопасности ПДн для ИСПДн соответствующего уровня защищенности и/или не покрывают всех угроз безопасности ПДн для данной ИСПДн.

3.4.10 Модернизация СЗПДн

Для функционирующих ИСПДн доработка (модернизация) СЗПДн должна проводиться в случае, если:

– изменился состав или структура самой ИСПДн, или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топология ИСПДн);

– изменился состав угроз безопасности ПДн в ИСПДн;

– изменился уровень защищенности ИСПДн.

Для определения необходимости доработки (модернизации) СЗПДн не реже одного раза в год должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и уровня защищенности ИСПДн. Проверка проводится сотрудниками IT-отдела РАМ имени Гнесиных. Результаты проверки оформляются актом и утверждаются ректором РАМ имени Гнесиных.

Уровень защищенности ПДн в ИСПДн определяется по нормативно-методическим документам ФСТЭК России, разрабатываемым во исполнение Требований к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119).

С целью своевременного выявления и предотвращения утечки ПДн по техническим каналам, исключения или существенного затруднения НСД и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности и доступности ПДн, в РАМ имени Гнесиных осуществляется периодический контроль за состоянием защиты ПДн.

Контроль осуществляется на основании Положения «О государственной системе защиты информации» и заключается в оценке:

– соблюдения нормативных и методических документов в области технической защиты ПДн;

– работоспособности применяемых средств защиты ПДн в соответствии с их эксплуатационной документацией;

– знаний и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

4 ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

4.1 Внутренний доступ

Доступ к персональным данным определяется в Перечне подразделений и сотрудников, допущенных к работе с ПДн, обрабатываемыми в ИСПДн РАМ имени Гнесиных.

Доступ к информационным ресурсам разграничивается в соответствии с Матрицей доступа к ИСПДн.

Разграничение прав доступа к ИСПДн возлагается на IT-отдел РАМ имени Гнесиных.

Уполномоченные лица имеют право получать только те ПДн, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

4.2 Внешний доступ (другие организации и граждане)

Сообщение сведений о ПДн другим организациям и гражданам разрешается при наличии письменного согласия субъекта и заявления, подписанного руководителем организации либо гражданином, запросившим такие сведения.

Предоставление ПДн без соответствующего согласия субъектов ПДн возможно в следующих случаях:

– в целях предупреждения угрозы жизни и здоровья субъекта ПДн;

– при поступлении официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскных мероприятиях»;

– при поступлении официальных запросов из Федеральной налоговой службы РФ, Пенсионного фонда России, Фонда социального страхования РФ, судебных органов;

– в других случаях, предусмотренных законодательством Российской Федерации.

Субъект, о котором запрашиваются сведения, должен быть уведомлён о передаче его ПДн третьим лицам, за исключением случаев, когда такое уведомление невозможно в силу форс-мажорных обстоятельств, а именно стихийных бедствий, аварий, катастроф и т. п..

Запрещается передача ПДн субъекта в коммерческих целях без его согласия.

5 КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПДн В РАМ ИМЕНИ ГНЕСИНЫХ

5.1 Общие правила

Контроль за соблюдением мероприятий по защите ПДн (далее — контроль) осуществляется с целью своевременного выявления и предотвращения утечки ПДн по техническим каналам, НСД к ним, преднамеренных программно-технических воздействий на ПДн, а также хищения ПДн.

Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты ПДн, решений ФСТЭК России, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите ПДн.

Постоянный контроль за состоянием защиты ПДн в РАМ имени Гнесиных осуществляет IT-отдел (лицо, назначенное приказом ректора).

Периодический контроль за деятельностью по защите ПДн в РАМ имени Гнесиных осуществляется комиссиями инспекции ФСТЭК России и Роскомнадзора.

Контроль за эффективностью применяемых в РАМ имени Гнесиных мер и средств защиты ПДн должен проводиться в соответствии с требованиями эксплуатационной документации на сертифицированные средства защиты, других нормативных документов не реже одного раза в год.

Обязательным является контроль за средствами защиты при вводе их в эксплуатацию, после проведения ремонта средств защиты, при изменении условий их расположения или эксплуатации.

5.2 Определение нарушений

Защита ПДн считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите ПДн является нарушением.

Нарушения по степени важности делятся на три категории:

– первая — невыполнение требований или норм по защите ПДн, в результате чего имелась или имеется реальная возможность их утечки по техническим каналам;

– вторая — невыполнение требований по защите ПДн, в результате чего создаются предпосылки к их утечке по техническим каналам;

– третья — невыполнение других требований по защите ПДн.

Нарушения для ИСПДн РАМ имени Гнесиных описываются в Модели угроз.

5.3 Порядок действий при обнаружении нарушений безопасности ПДн

5.3.1 При обнаружении нарушений первой категории

При обнаружении нарушений первой категории руководители подразделений обязаны:

– немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению;

– организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

– сообщить в ФСТЭК России о вскрытых нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений, проверки достаточности и эффективности принятых мер. Контроль за устранением этих нарушений осуществляется IT-отделом.

5.3.2 При обнаружении нарушений второй и третьей категорий

При обнаружении нарушений второй и третьей категорий руководители подразделений обязаны принять необходимые меры по их устранению в соответствии с ОРД.

Контроль за устранением этих нарушений осуществляется IT-отделом.

5.3.3 Разбирательство

Разбирательство и составление заключений в обязательном порядке должно проводиться в случае выявления следующих фактов:

– несоблюдение условий хранения носителей ПДн;

– использование средств защиты ПДн, применение которых может привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) ПДн или к снижению уровня защищенности ПДн;

– нарушение заданного уровня безопасности ПДн (конфиденциальность/ целостность/доступность).

В ходе разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

По окончании разбирательства необходимо провести разработку (доработку) и принятие мер по предотвращению повторения подобных нарушений.

Для проведения разбирательства инцидентов утечки ПДн необходимо разработать Регламент проведения расследования утечки ПДн.